Model # AR410W

USER'S MANUAL

Ver. 1A

Table of Contents

1. Overview 4
   1.1 Product Features 4
   1.2 System Requirements 4
   1.3 Applications 4
2. Getting Started 5
   2.1 Knowing the 802.11g Wireless Router 5
2.2 Connecting to the Wireless Router 5
   2.2.1 Connecting the Router 5
   2.2.2 Verify Connection to Router 7
   2.2.3 Configuring the Router 9
3. Verifying Internet Connection 17
4. Web Configuration Utility 18
   4.1.1 LAN & DHCP Server 18
   4.1.2 WAN 19
   4.1.3 Password 20
   4.1.4 Time 20
   4.1.5 Dynamic DNS 21
4.2 Wireless 22
   4.2.1 Basic 22
   4.2.2 Authentication 23
   4.2.3 Advanced 25
4.3 Status 26
   4.3.1 Device Information 26
   4.3.2 Log 27
   4.3.3 Log Setting 28
   4.3.4 Statistic 29
   4.3.5 Wireless 29
4.4 Routing 30
   4.4.1 Static 30
   4.4.2 Dynamic 31
   4.4.3 Routing Table 32
4.5 Access 33
   4.5.1 MAC Filters 33
   4.5.2 URL Blocking 34
   4.5.3 IP Filter 35
   4.5.4 Domain Blocking 36
   4.5.5 Protocol Filter 37
   4.5.6 Virtual Server 38
   4.5.7 Special AP 39
   4.5.8 DMZ 40
   4.5.9 Firewall Rule 41
4.6 Management 42
   4.6.1 SNMP 42

4.6.2 Remote Management 43
4.7 Tools 44
4.7.1 Restart 44
4.7.2 Settings 45
4.7.3 Firmware 45
4.7.4 Ping Test 46
5. Troubleshooting 47
Appendix 48

1. Overview

1.1 Product Features

● Compliance with IEEE 802.11g and 802.11b standards
● Highly efficient design mechanism to provide unbeatable performance
● Strong network security with WEP and WPA-PSK encryption
● Achieving data rate of up to 54Mbps for 802.11g and 11Mps for 802.11b; optional 108Mbps is achievable with compatible wireless network adapters
● Quick and easy setup with Web-based management utility

1.2 System Requirements

● Windows 98, 98SE, Millennium Edition (ME), 2000 and XP operating systems
● Microsoft Internet Explorer 6.0 or higher
● DSL/Cable Modem Broadband Internet connection and ISP account
● PCs equipped with 10Mbps or 10/100 Mbps Ethernet connection to support TCP/IP protocol

1.3 Applications

● Home SOHO networking for device sharing and wireless multimedia
● Wireless office provides a wider range for home and SOHO Ethernet
● Enables wireless building-to-building data communication
● Built-in infrastructure mode
● Router provides ideal solution for:
● Difficult-to-wire environments
● Temporary LANs for scenarios such as trade-exhibitions and meetings
● Enables LAN adaptability to frequently changing environments
● Enables remote access to corporate network information, for example e-mail and the company home page

2. Getting Started

2.1 Knowing the 802.11g Wireless Router

Ports:
(LAN Ports): automatically detect the cable type when connecting to Ethernet-enabled computers.
(WAN Port): the connection for the Ethernet cable to the cable or DSL modem.
(Power): receptor for the power adapter
(Reset): restore the router to its original factory default.

LEDs:

LED	Color	Status	Description
Power	Green	On	Receiving power from power supply
		Off	Not receiving power
Status	Green	On	Device is ready
WAN	Green	On	Device is connected to WAN
		Blinking	Data transmission
WLAN	On		Link ready
	On	Blinking	Data transmission
	Off		Link not ready
LAN	On		Link is established
	On	Blinking	Data transmission
	Off		Link not established

2.2 Connecting to the Wireless Router

2.2.1 Connecting the Router

Note: Prior to connecting the router, be sure to power off your computer, DSL/Cable modem, and the router. You should setup the router with a wired connection first before attempting to setup any wireless connection.

Step 1 Connect one end of a network cable to the **WAN** port of the router and connect the other end of the cable to the DSL/Cable modem.

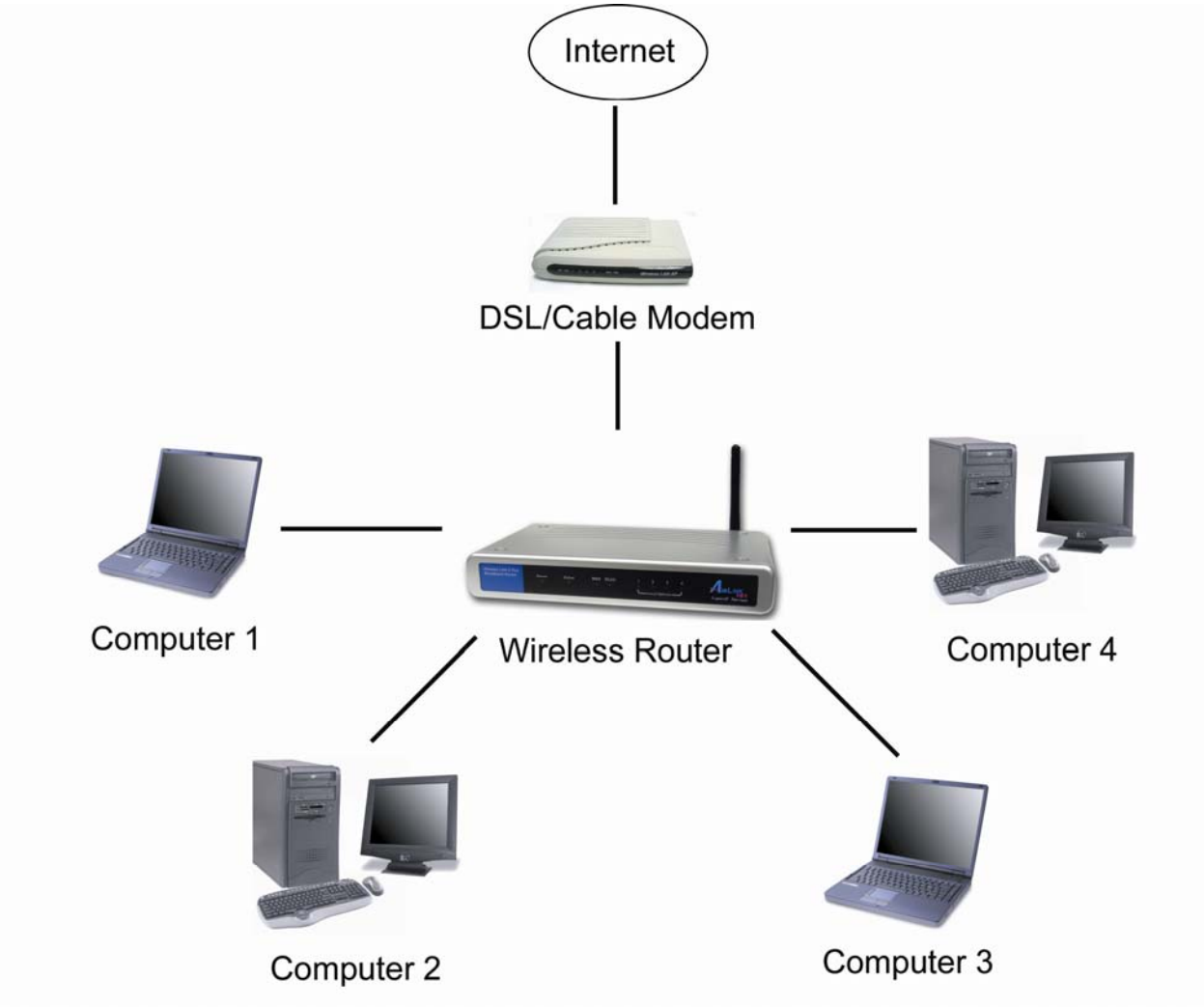
Step 2 With another network cable, connect one end of the cable to your computer's network card and connect the other end to one of the **LAN** ports of the router.

Step 3 Power on the DSL/Cable modem and wait for the lights on the modem to settle down.

Step 4 Power on the router by connecting one end of the supplied power adapter to the power jack of the router and connecting the other end to an electrical outlet.

Step 5 Power on your computer.

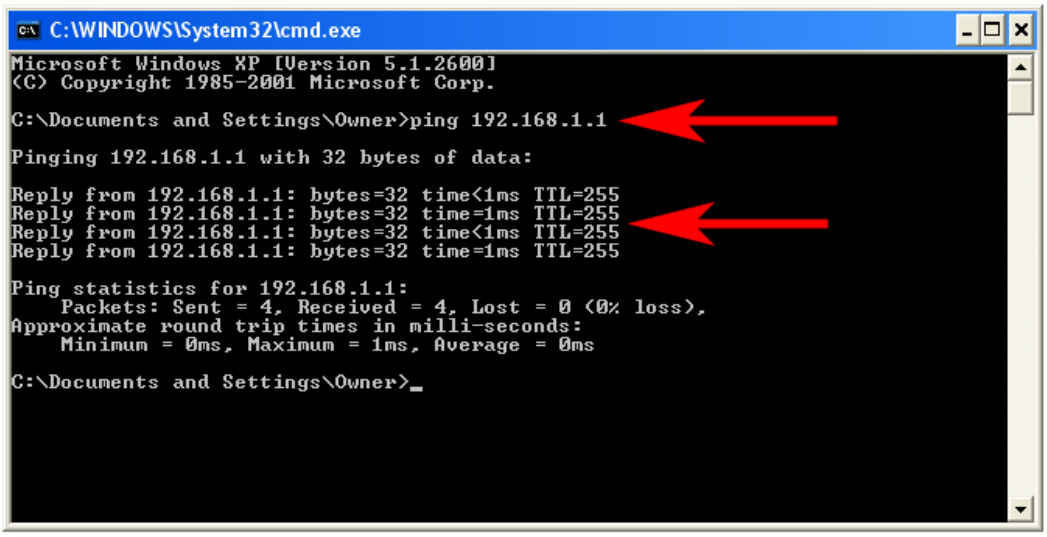
Step 6 Make sure the **WAN**, **WLAN**, and the **LAN** ports that the computer is connected to are lit. If not, try the above steps again.



2.2.2 Verify Connection to Router

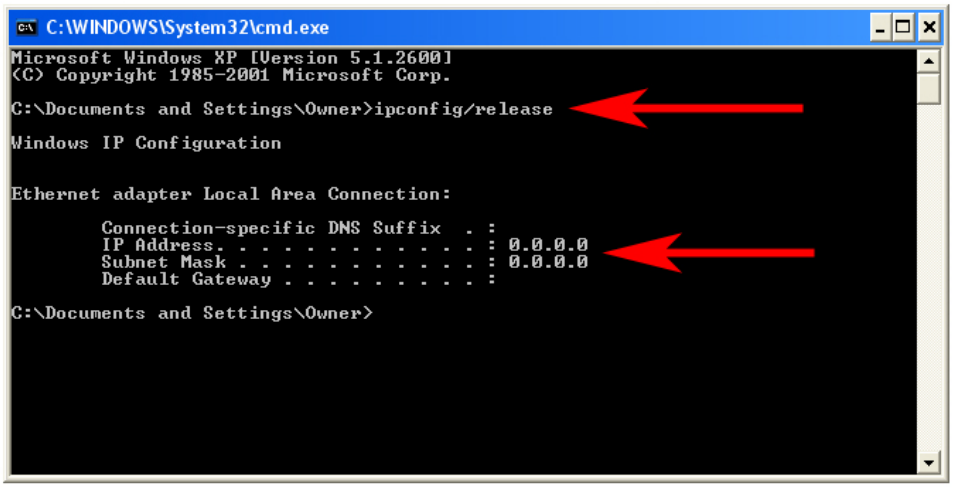
Step 1 Go to **Start**, **Run**, type **command** (for Windows 95/98/ME) or **cmd** (for Windows 2000/XP) and click **OK**. You will see the command prompt as below.

Step 2 Type **ping 192.168.1.1** and press **Enter**. You should get four reply responses back.

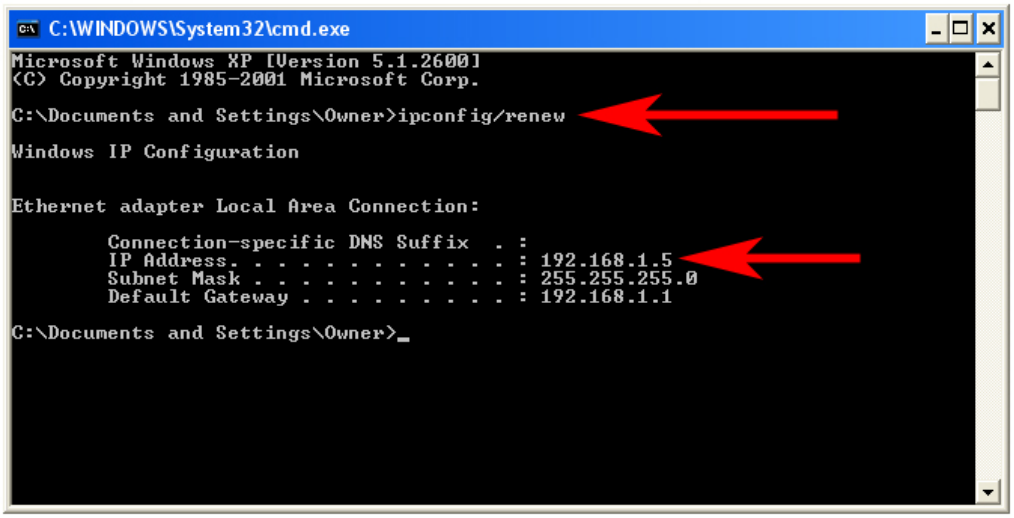

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Owner>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Documents and Settings\Owner>_

Step 3 If you get **Request timed out**, or **Destination host unreachable**, double-check the network cable connection between the computer and the router and try **Step 2** again. If you still encounter problem, go to the next step; otherwise proceed to the next section.

Step 4 For Windows 2000/XP, type **ipconfig/release** and press **Enter**.

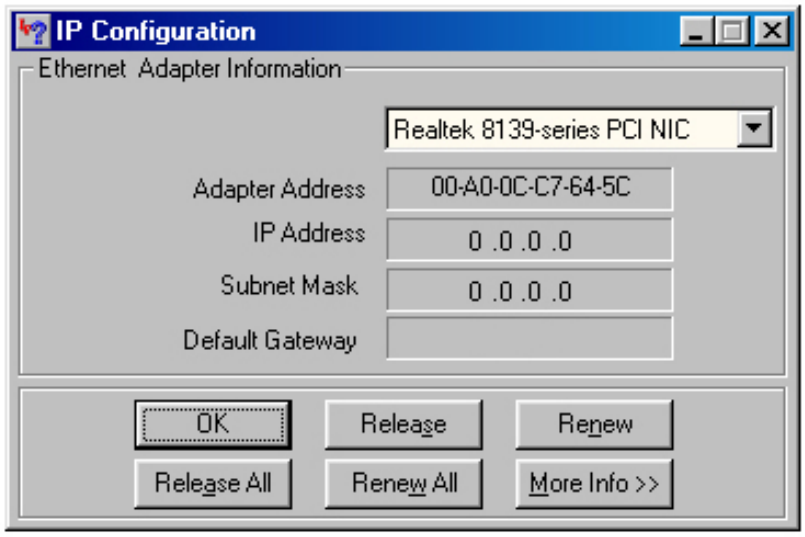

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Owner>ipconfig/release
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :
C:\Documents and Settings\Owner>

Step 5 Type **ipconfig/renew** and press **Enter**. You should get an IP address of **192.168.1.x** (where **x** is a number between 2 – 254). Proceed to the next section. If you don't get an IP address, reset the router by holding in the reset button at the back of the router for 10 seconds while it is ON and try **ipconfig/renew** again.

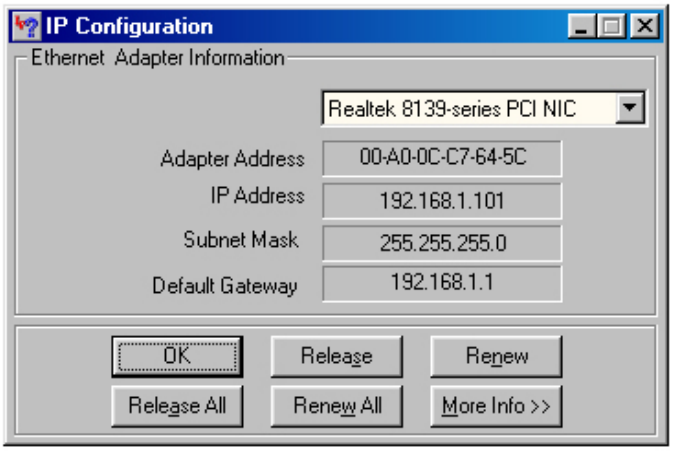

C:\WINDOWS\System32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Owner>ipconfig/renew
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\Owner>_

Step 6 For Windows 95/98/ME go to **Start**, **Run**, type **winipcfg** and click **OK**.

Step 7 Select your network card from the drop-down menu and click **Release**.

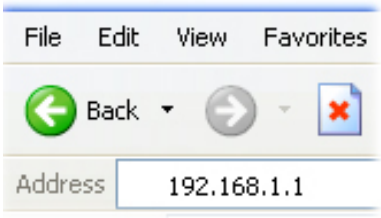


Step 8 After your IP address is released, click **Renew**. You should get an IP address of **192.168.1.x** (where **x** is a number between 2 – 254). If you don't get an IP address, reset the router by holding in the reset button at the back of the router for 10 seconds while it is ON and try **Renew** again.

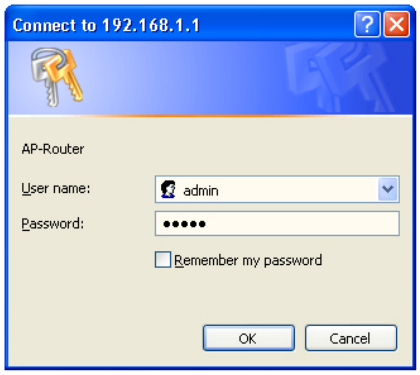


2.2.3 Configuring the Router

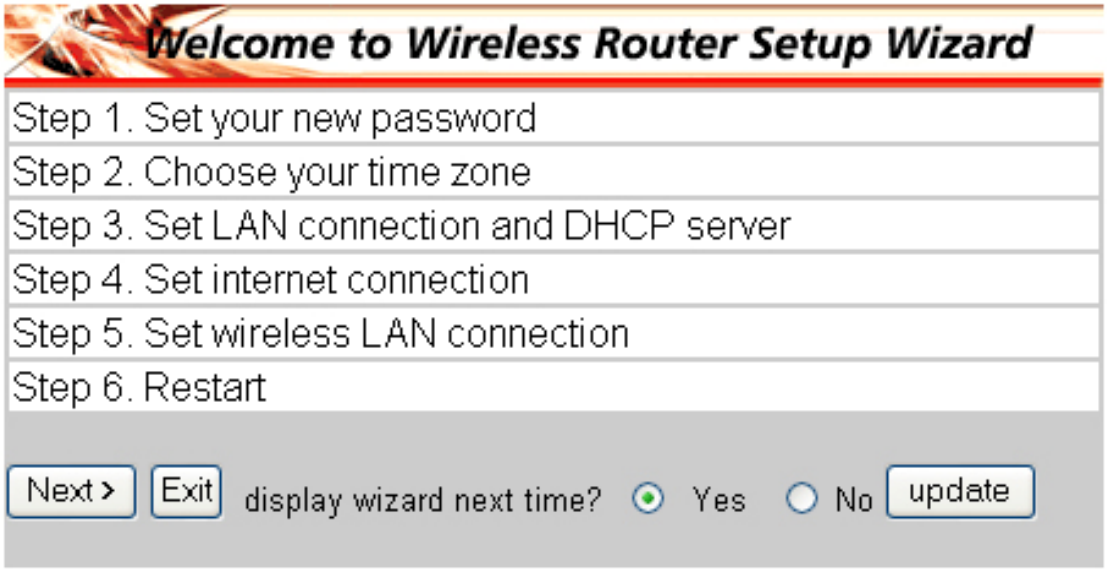
Step 1 Open the web browser and type **192.168.1.1** in the URL Address field and press **Enter**.



Step 2 Enter **admin** for both the username and the password fields and click **OK**.

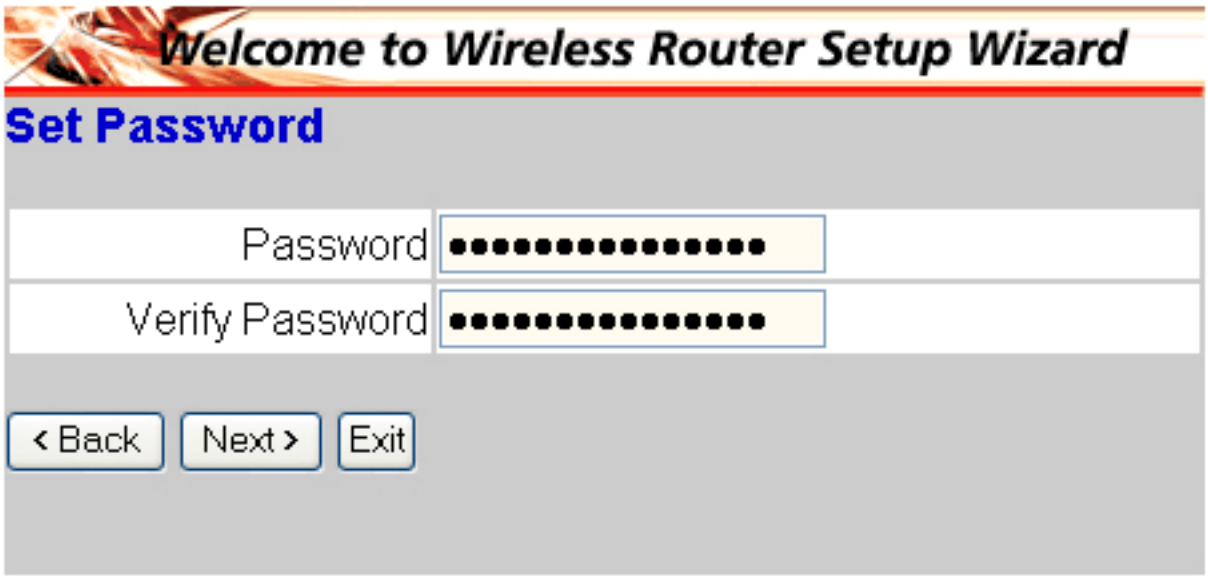


Step 3 Click **Next** at the router's Setup Wizard.

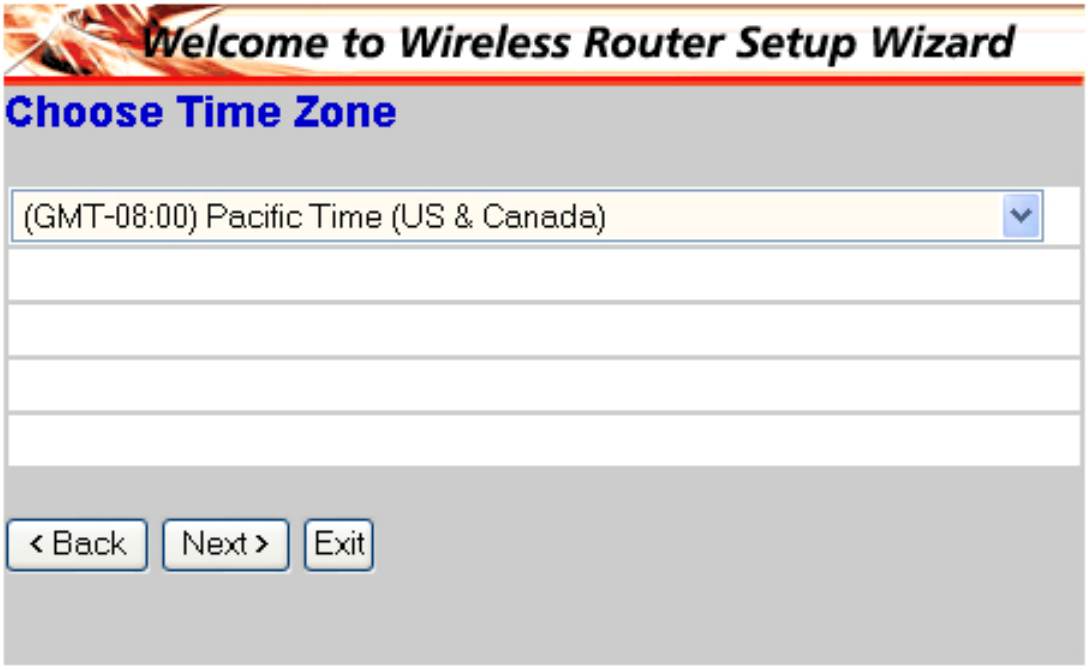


Note: If you don't see the Setup Wizard, click on the Wizard button on the menu bar.

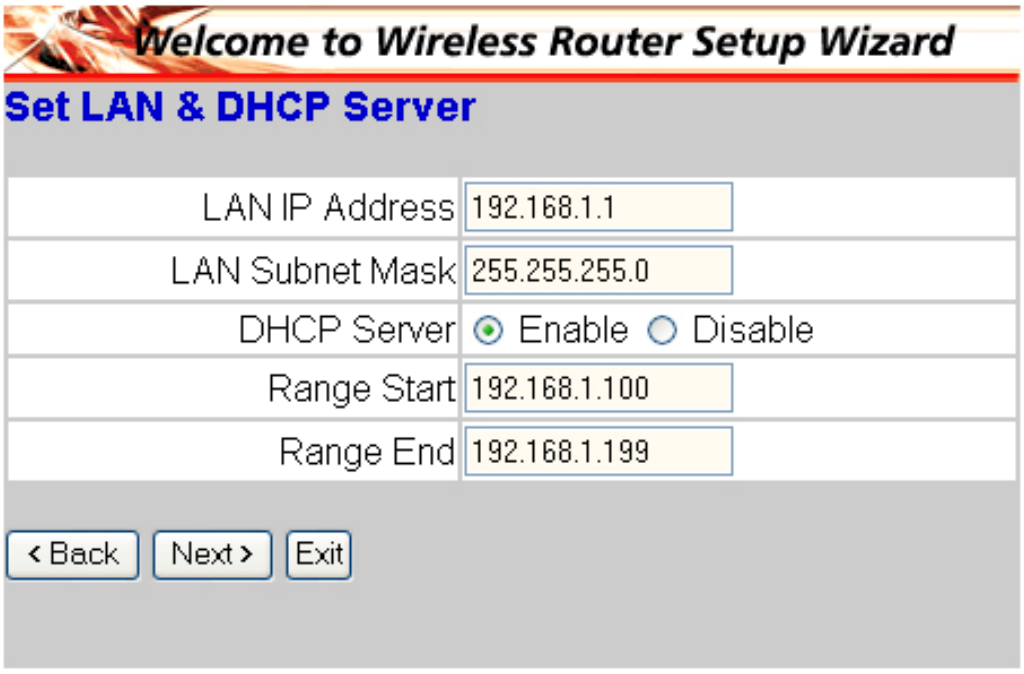
Step 4 Change the router's password by removing the bullets and typing in your new password. **OR** you may keep the current password (**admin**) and click **Next**.



Step 5 Select your time zone and click **Next**.

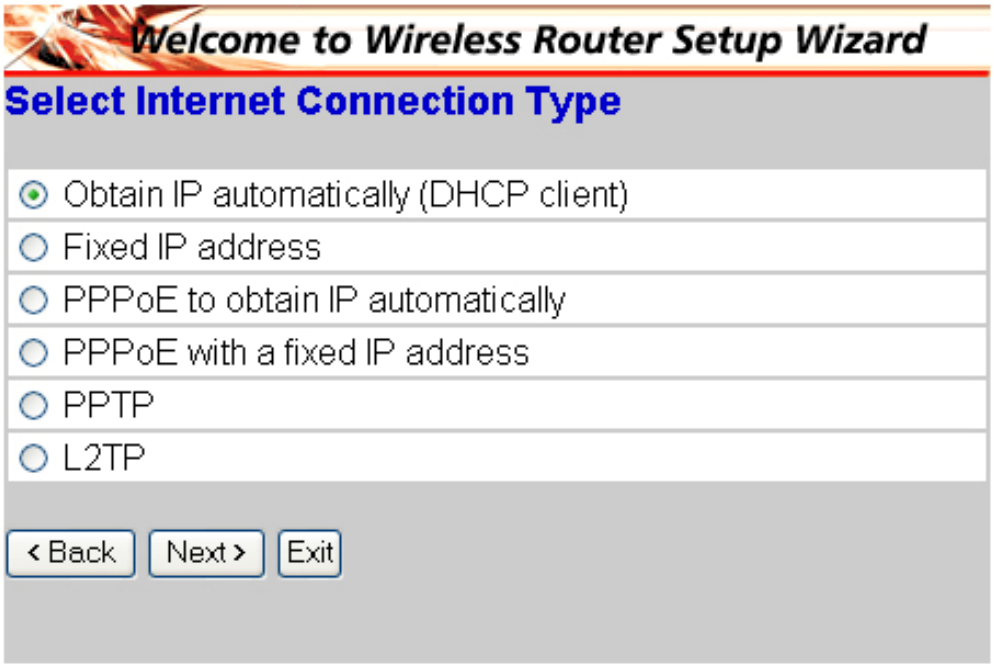


Step 6 You may change the router's LAN settings or just click **Next** to keep the default settings.

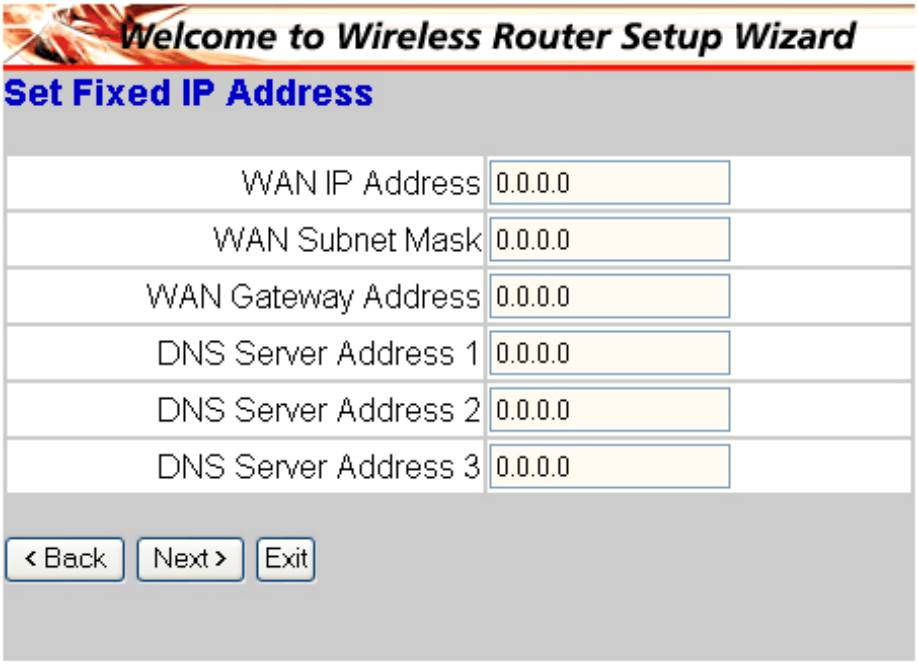


Step 7 The router will now auto-detect what type of WAN setting your DSL/Cable modem has. You may follow steps 8a through 8f to configure your WAN type.
Note: If you are certain that your WAN type is different then from the one detected, you should manually select the proper WAN type to configure.

Step 8a For **Obtain IP automatically (DHCP client)** and **cable modem** users click **Next** and proceed to **Step 9**.

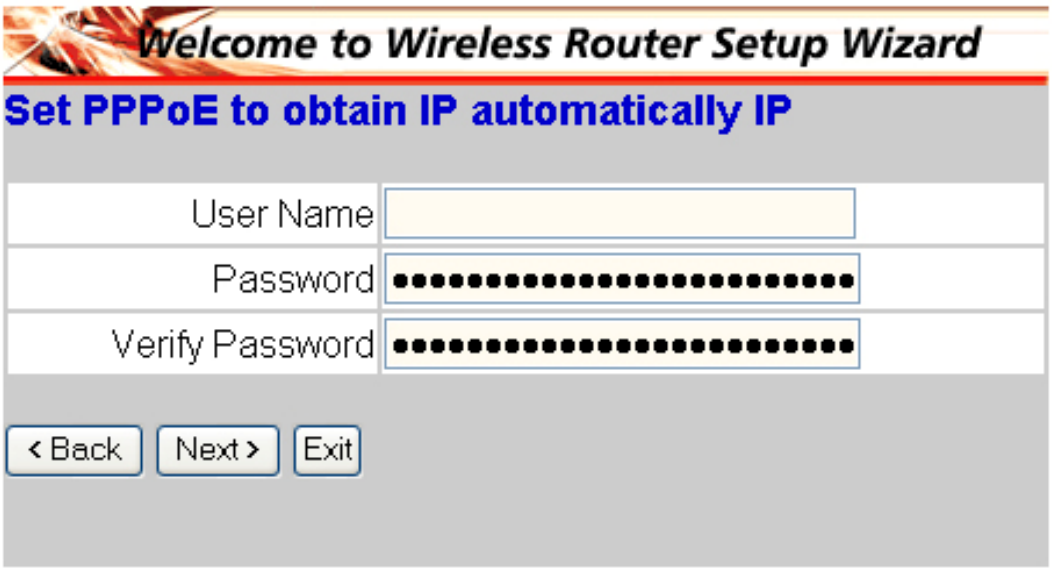


Step 8b For **Fixed IP address**, enter the values provided by your ISP and click **Next**. Proceed to **Step 9**.



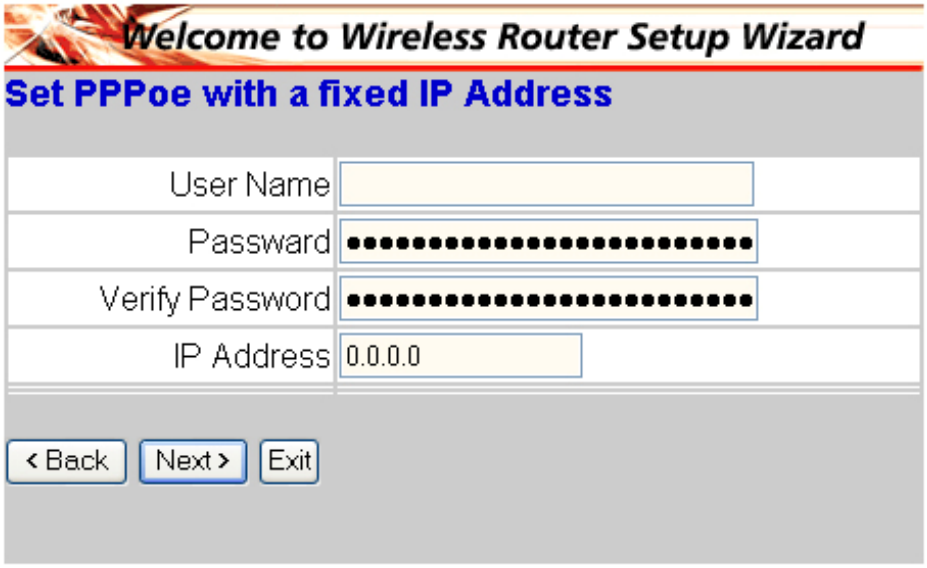
Step 8c For **PPPoE to obtain IP automatically**, enter the User Name and Password required to get online and click **Next**. Proceed to **Step 9**. You may need to include the domain name with your user name.

Ex. **username@sbcglobal.net**

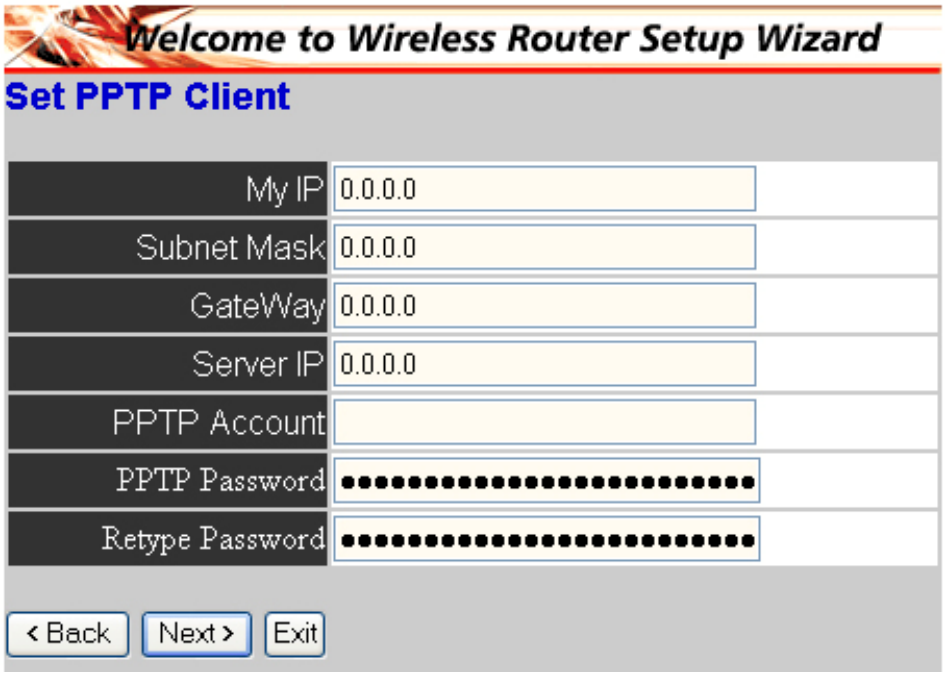


Step 8d For **PPPoE with a fixed IP address**, enter the User Name and Password required to get online and the IP address provided by your ISP, and click **Next**. Proceed to **Step 9**. You may need to include the domain name with your user name.

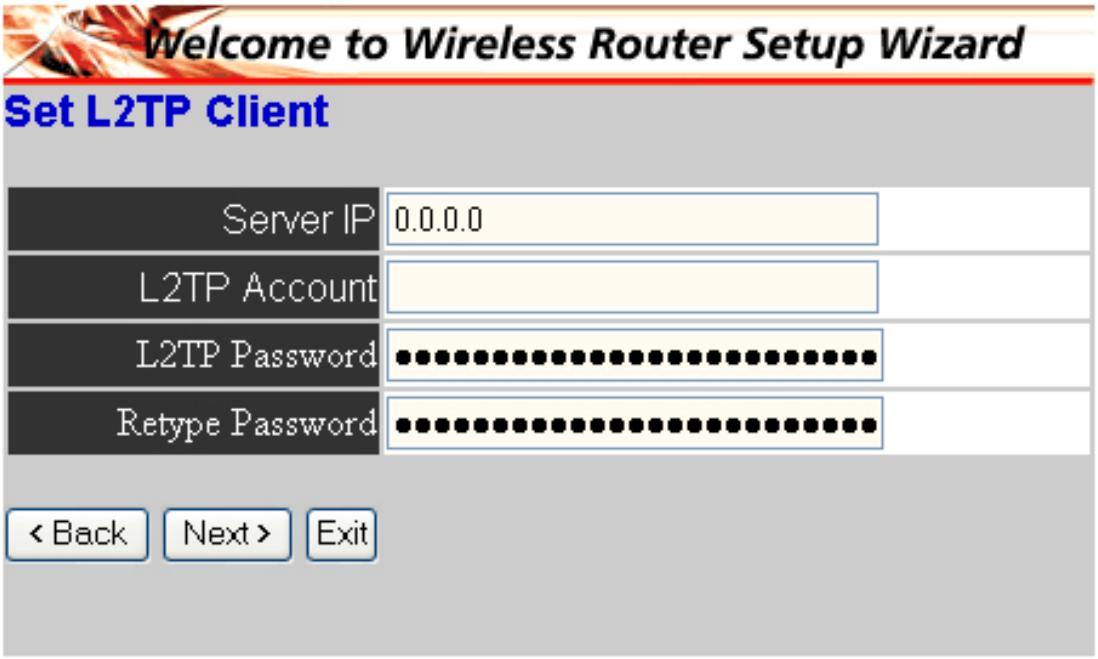
Ex. **username@sbcglobal.net**



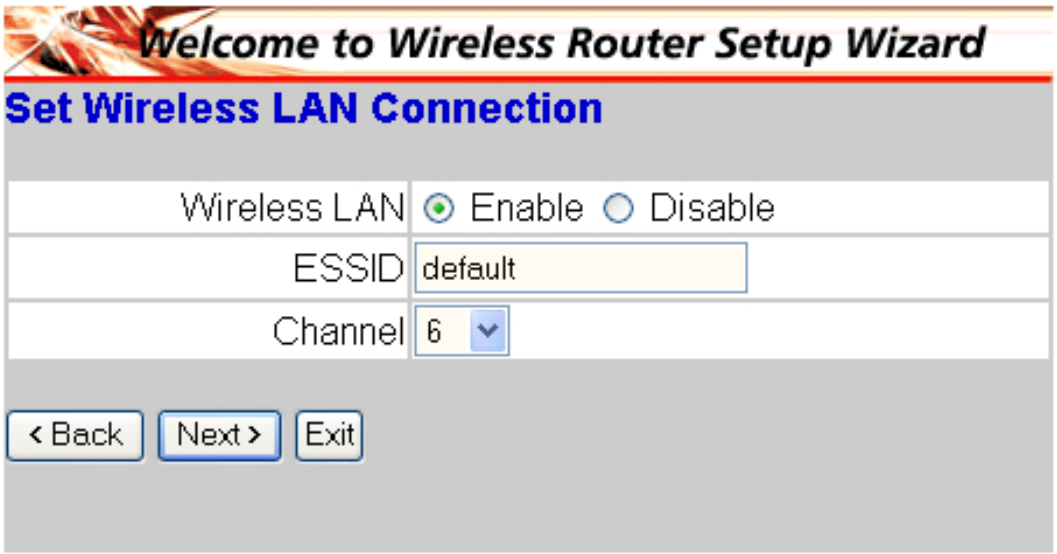
Step 8e For **PPTP**, enter the values provided by your ISP and click **Next**. Proceed to **Step 9**.



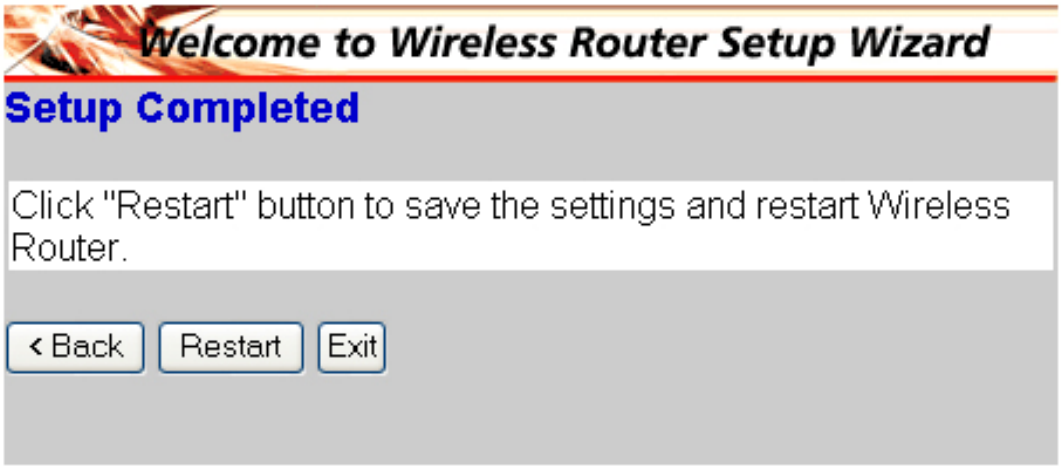
Step 8f For **L2TP**, enter the values provided by your ISP and click **Next**.



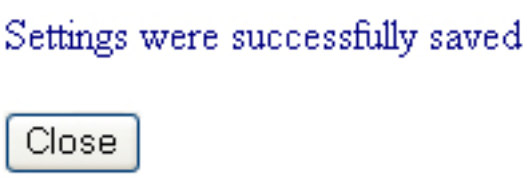
Step 9 Choose to **Enable** or **Disable** the wireless function of the router. Click **Next** to accept the default Wireless Network ID (**default**) or change the existing name to fit your current wireless network. You may also change the channel number if needed.7



Step 10 Click **Restart** to apply the settings.



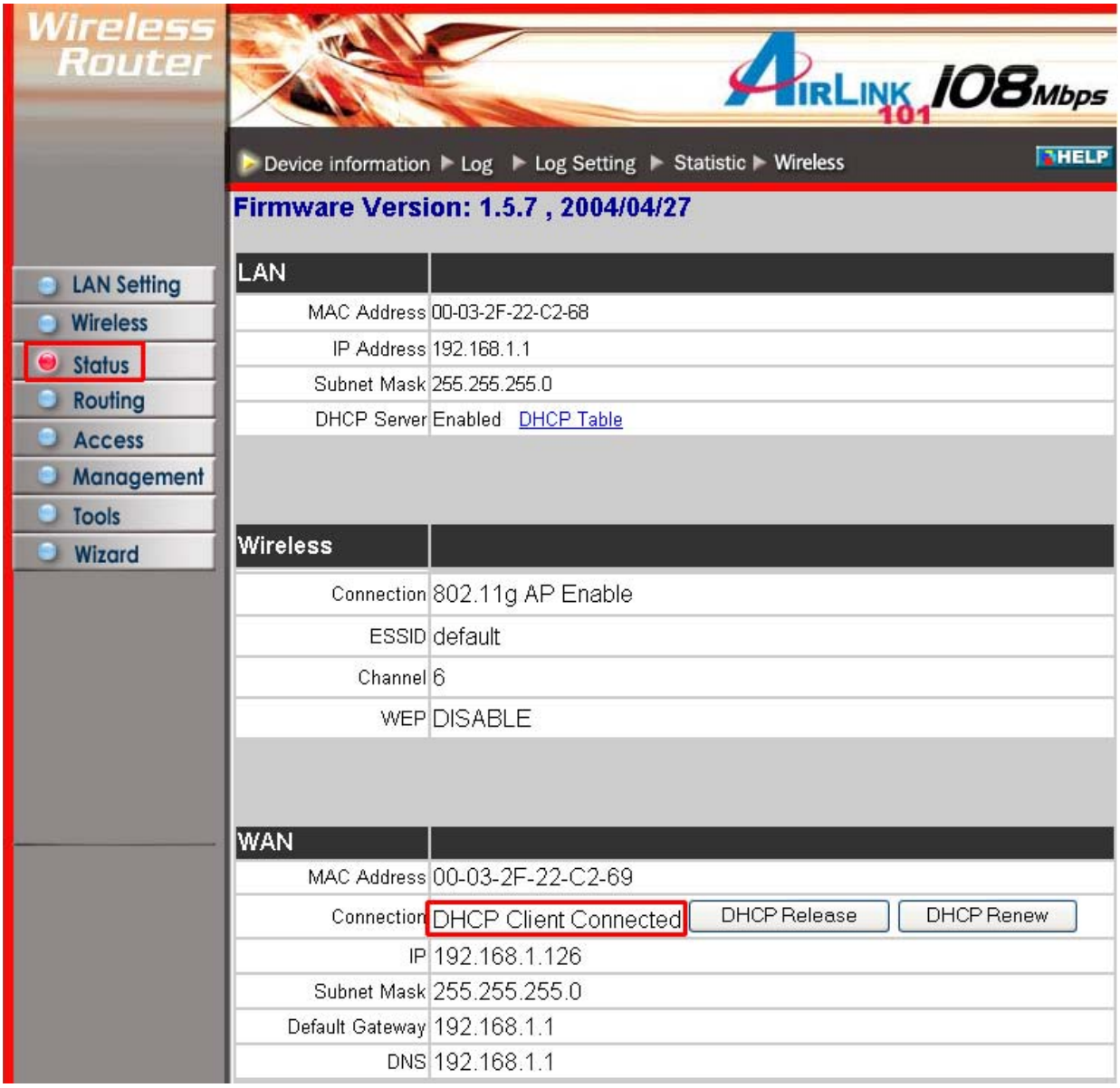
Step 11 Click **Close** and close the web browser.



3. Verifying Internet Connection

Step 1 Login to the router's configuration page and click on the **Status** button.

Step 2 Verify that the status for the **WAN** connection says **Connected**.



Note: If the status is disconnected, click on **DHCP Renew** (for Cable Modem), or **Connect** (for DSL Modem). If it is still disconnected, go to the **Troubleshooting** section at the end of this manual.

Step 3 If the status says **Connected**, your setup is complete.

4. Web Configuration Utility

Step 1 Open the web browser and type **192.168.1.1** in the URL Address field and press **Enter**.

Step 2 Enter **admin** for both the username and the password fields and click **OK**.

4.1.1 LAN & DHCP Server

This page enables you to set the LAN and DHCP properties such as the host name, IP address, subnet mask, and the domain name. LAN and DHCP profiles are listed in the DHCP table at the bottom of the screen.

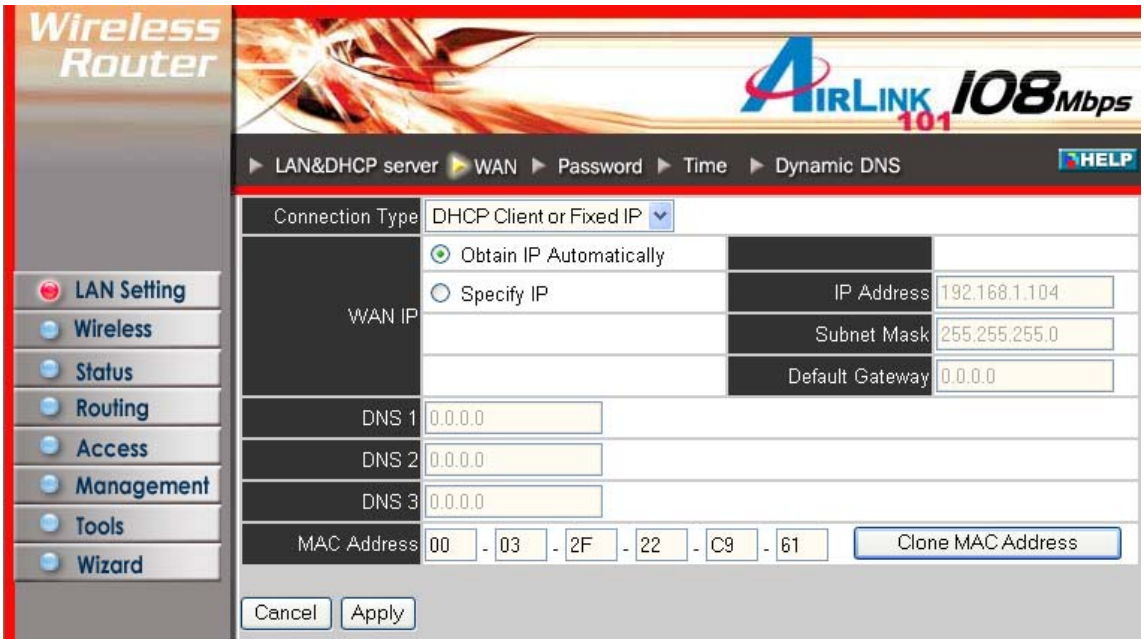
Host Name: Type the host name (if available) in the text field. The host name is provided by your ISP and is required by some ISPs for Internet connection.
IP Address: This is the IP address of the router. The default IP address is **192.168.1.1**. You may change it to suit your existing LAN environment.
Subnet Mask: Type the subnet mask for the router in the text field. The default subnet mask is **255.255.255.0**.
DHCP Server: Enables the DHCP server function which allows the router to automatically assign IP addresses to devices connected to the LAN. DHCP is enabled by default. All DHCP clients are listed in the table at the bottom of the screen, providing the host name, IP address, and MAC address of each client.
Start IP: Enter an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

End IP: Enter an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.
Domain Name: Enter the local domain name of the network in the text field. This field is optional.
Lease Time: Set the lease time for the IP address assigned by the router.

Click **Apply** to save any changes.

4.1.2 WAN

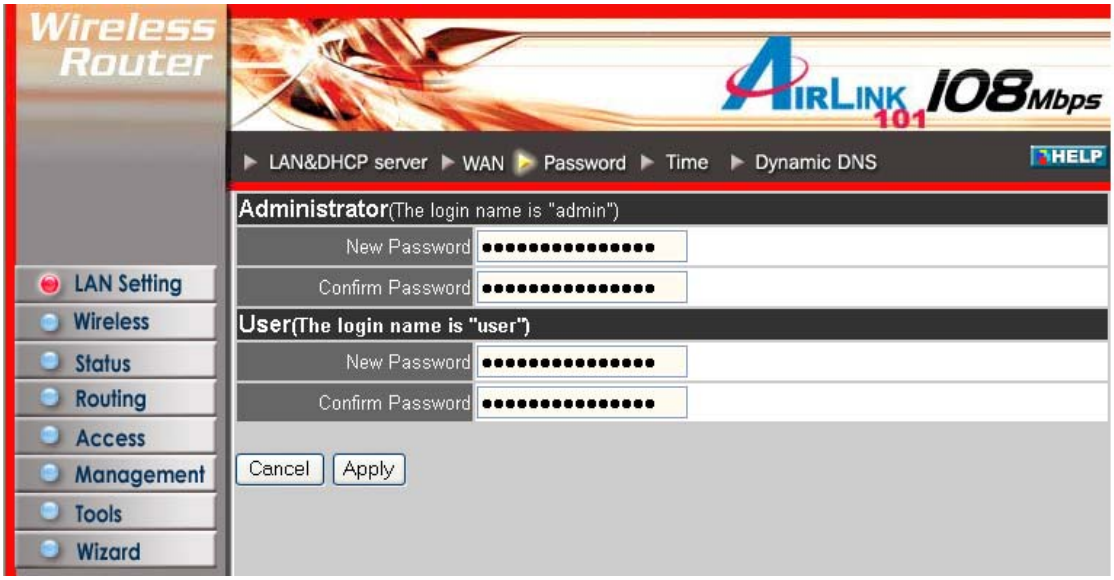
This screen enables you to set up the router's WAN connection, specify the IP address for the WAN port, add DNS address, and enter the MAC address.



Connection Type: Select your Internet connection type: DHCP client, PPPoE, PPTP, or L2TP from the drop-down list.
WAN IP: Select whether you want to specify an IP address manually, or use DHCP to obtain an IP address automatically from your ISP. When *Specify IP* is selected, type the IP address, subnet mask, and default gateway in the text fields. Your ISP will provide you with the information.
DNS 1/2/3: Enter up to three DNS IP address in the text fields. Your ISP will provide you with the information.
MAC Address: If your ISP requires a registered MAC address, click on **Clone MAC Address** to clone your PC's MAC Address.

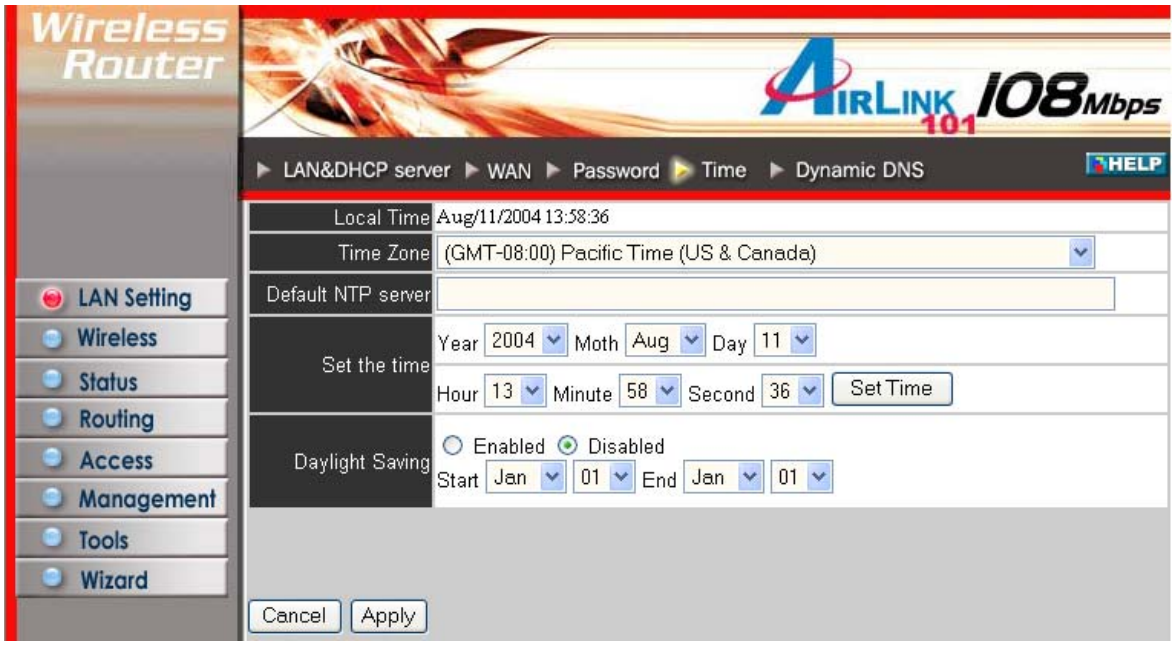
4.1.3 Password

This screen enables you to set administrative and user passwords. These passwords are used to gain access to the router's interface. The User account can only view the settings but not change them. To change the settings, you must log in using the admin account.



4.1.4 Time

This screen enables you to set the time and date for the router. Select your time zone and enable or disable daylight saving.

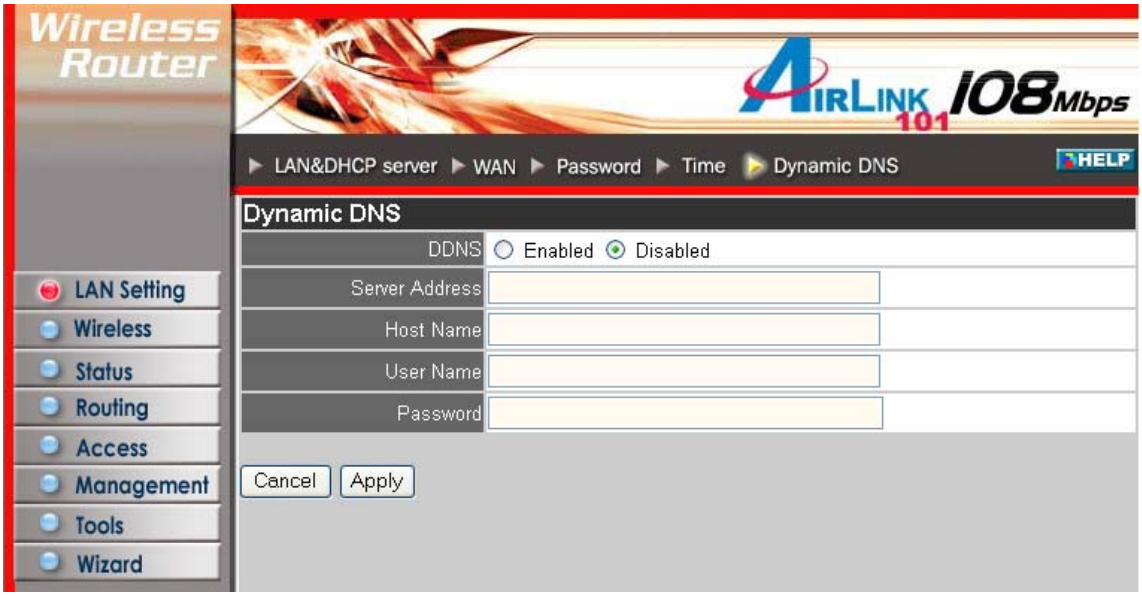


Local Time: Displays the local time and date.
Time Zone: Select your time zone from the drop-down list.
Default NTP server: Enter a public NTP time server (optional)
Daylight Saving: Allows you to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

4.1.5 Dynamic DNS

DDNS allows Internet users to connect to your Virtual Servers using an URL, rather than an IP Address.

Note: You must register for the DDNS service at one of the DDNS Service Providers first.



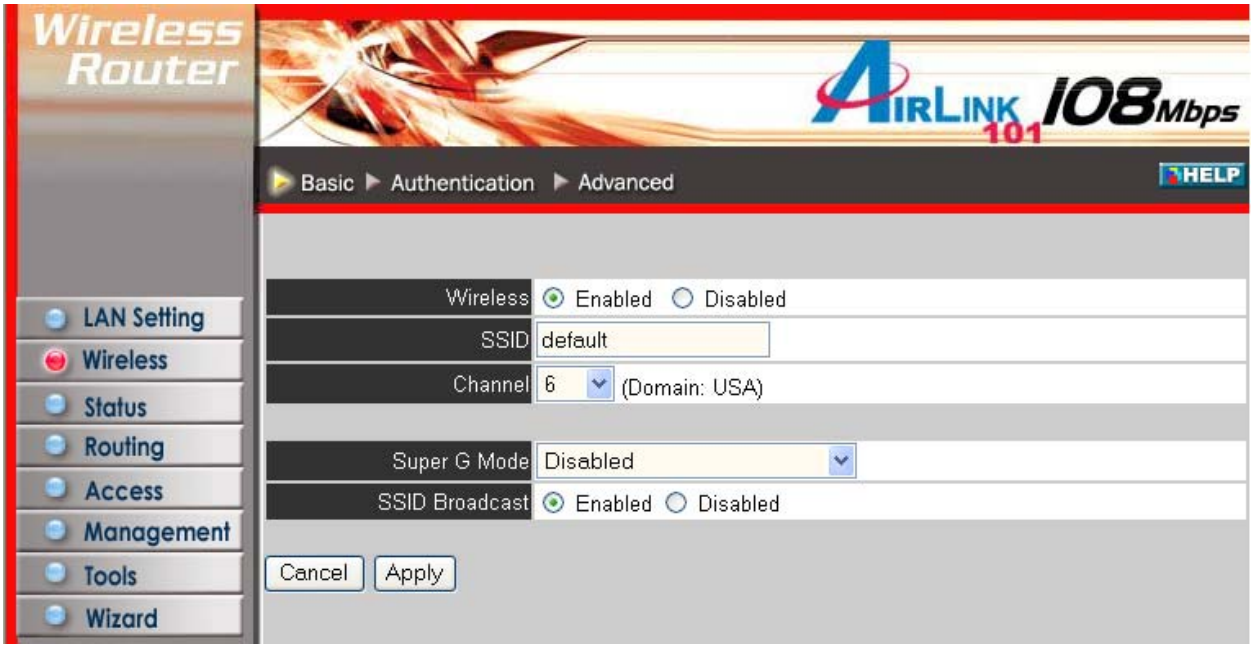
Server Address: Enter the IP Address of the DDNS server.
Host name: enter your host name.
User name: enter your user name for the DDNS service.
Password: enter your password for the DDNS service.

4.2 Wireless

This section enables you to set wireless communications parameters for the router's wireless LAN feature.

4.2.1 Basic

This page allows you to enable and disable the wireless LAN function, change the SSID, and select the channel for wireless communications.



Enable/Disable: Enables and disables wireless LAN via the router. If disabled, no wireless clients can connect to the router.
SSID: Type an SSID in the text field. The default SSID is **default**. The SSID of any wireless clients must match the SSID typed here in order for the wireless clients to access the router.
Channel: Select a transmission channel for wireless communications. The channel of any wireless clients must match the channel selected here in order for the wireless clients to access the router.
Super G Mode: Super G is a group of performance enhancement features that increase end user application throughput in an 802.11g network. Super G is backwards compatible with standard 802.11g devices. For best performance, all wireless devices on the network should be Super G capable. Select either **Disabled**, **Super G without Turbo**, **Super G with Dynamic Turbo**, or **Super G with Static Turbo**.

Note:

- **Super G without Turbo:** Capable of Packet Bursting, Fast Frames, Compression, and no Turbo mode.
- **Super G with Dynamic Turbo:** Capable of Packet Bursting, Fast Frames,

Compression, and Dynamic Turbo. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are configured with Super G with Dynamic Turbo enabled.

Super G with Static Turbo: Capable of Packet Bursting, Fast Frames, Compression, and Static Turbo. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all the devices on the wireless network are configured with Super G with Static Turbo enabled.

SSID broadcast: select to enable or disable the broadcast of the router's SSID.

4.2.2 Authentication

This screen enables you to set authentication type for secure wireless communications. Open System allows public access to the router via wireless communications. Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key. This router also supports WPA-PSK encryption.

Authentication Type: The default setting for authentication is set to Open System. There are five options: Open System, Shared Key, WPA, and WPA-PSK.

Note: If you don't have a RADIUS server in your network and you want to use WPA encryption, select WPA-PSK as the Authentication Type.

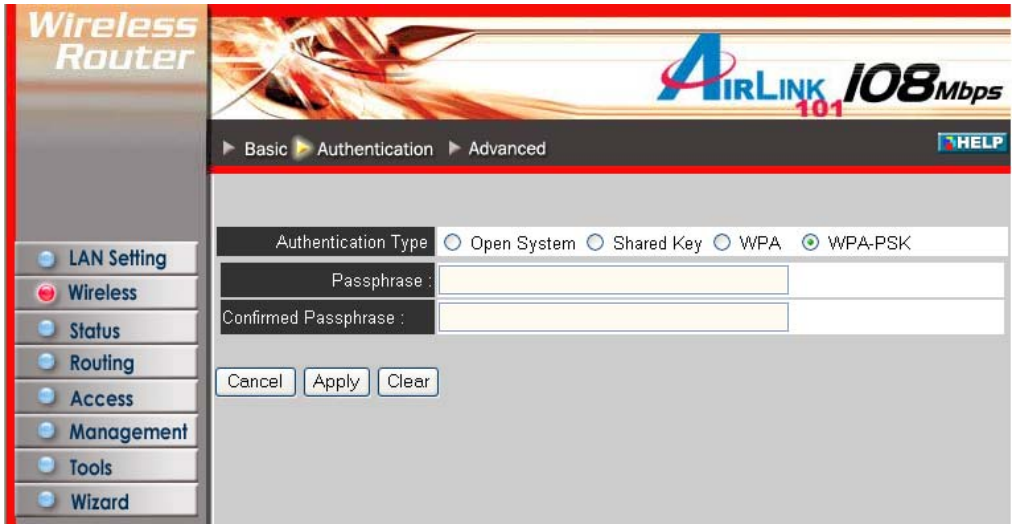
WEP: Enabled or Disabled. This is to enable or disable WEP encryption.
Mode: Select the key mode in **ASCII** (any letter or number) or **HEX** (letters A-F and numbers 0-9).

WEP Key: Select the level of encryption you want from the drop-down list. The router supports, 64-bit (Hex 10 characters/ASCII 5 characters) and 128-bit encryption (Hex 26 characters/ASCII 13 characters).

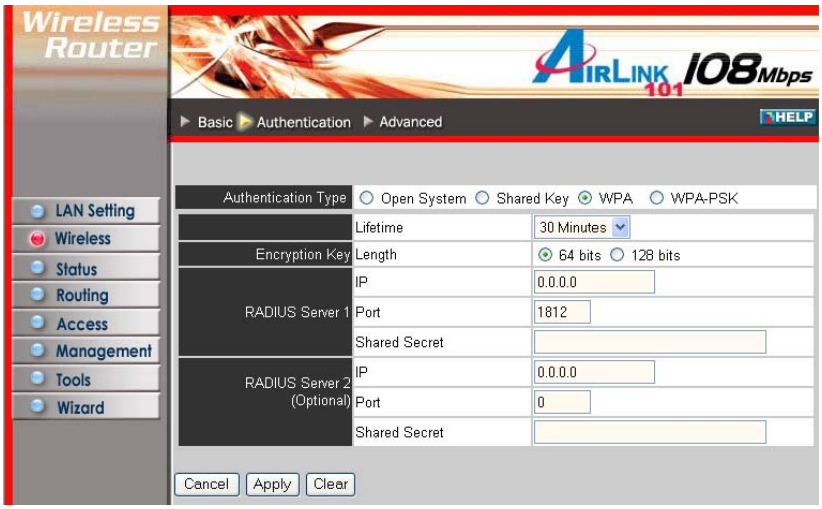
Example: if you selected to use **64-bits** using **HEX** characters, you would enter **10** Hex characters in each of the four keys below.

Key 1 ~ Key 4: Enter a value for each key. Use the radio button to select which key you want to activate. All wireless clients must use the same key number with the identical value. Click **Clear** to erase key values.

If you choose **WPA-PSK** as the Authentication Type, enter the PSK key in the Passphrase field. The length for the passphrase should be 8 to 63 characters (ASCII).



For **WPA** users, enter the RADIUS server's IP address as well as all the necessary encryption settings.



4.2.3 Advanced

This screen enables you to configure advanced wireless functions.

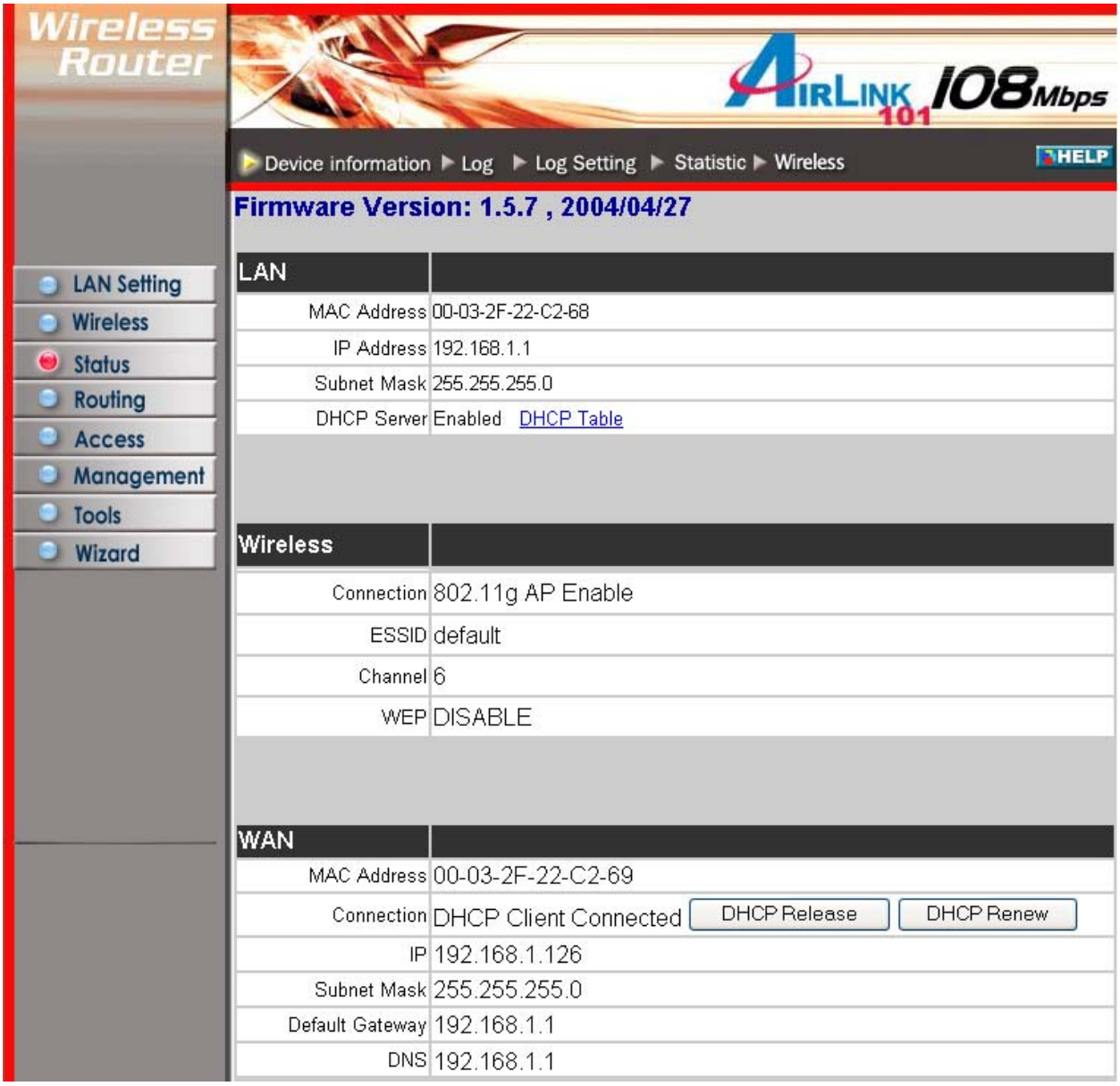
Beacon Interval: Type the beacon interval in the text box. You can specify a value from 1 to 1000. The default beacon interval is 100.
RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2432 until data flow is normalized.
Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 256 and 2432 until packet transfer rates are minimized. (***NOTE***: *setting the fragmentation threshold value may diminish system performance*.)
DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. You can specify a value between 1 and 65535. The default value is 3.
TX Rates (Mbps): Select one of the wireless communications transfer rates, measured in megabits per second, based upon the speed of wireless adapters connected to the WLAN.
11g Only Mode: If enabled, the router will only communicate in 11g mode (54 Mbps).
Antenna Transmit Power: select from full, half, quarter, eighth, min.

4.3 Status

This selection enables you to view the status of the router's LAN and WAN connections, and view logs and statistics pertaining to connections and packet transfers.

4.3.1 Device Information

This screen enables you to view the router's LAN, Wireless, and WAN configuration.



Firmware Version: Displays the current version of the firmware installed. After updating the firmware from **Tools - Firmware**, check this page to ensure that your firmware is successfully updated.
LAN: This field displays the router's LAN interface MAC address, IP address, subnet mask, and DHCP server status. Click *DHCP Table* to view a list of clients currently connected to the router LAN interface.
Wireless: Displays the router's wireless connection information, including the router's wireless interface MAC address, the connection status, the SSID, the channel number, and whether WEP encryption is enabled or disabled.
WAN: This field displays the router's WAN interface MAC address, DHCP client status, IP address, subnet mask, default gateway, and DNS. Click ***DHCP Release*** to release the IP address obtained by the router from the ISP. Click ***DHCP Renew*** to renew the IP address obtained by the router from the ISP.

Note: The buttons will be changed to **Connect** and **Disconnect** if you've set the router to one of the PPPoE modes, but the functions remain the same.

4.3.2 Log

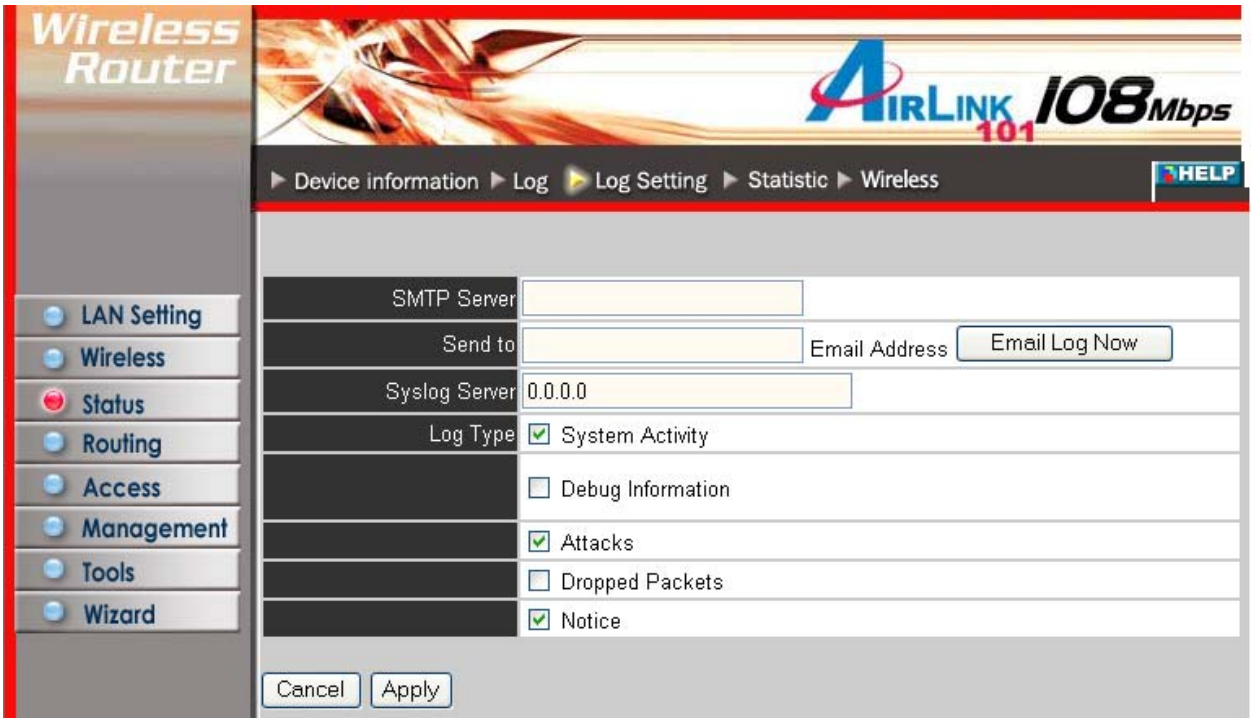
This screen enables you to view a log of the router's system statistics, events, and activities. The log can display up to 200 entries. Older entries are overwritten by new entries. The Log screen commands are as follows:

Click ***First Page*** to view the first page of the log
Click ***Last Page*** to view the final page of the log
Click ***Previous Page*** to view the page just before the current page
Click ***Next Page*** to view the page just after the current page
Click ***Clear Log*** to delete the contents of the log and begin a new log

Click ***Refresh*** to renew log statistics
Time: Displays the time and date that the log entry was created.
Message: Displays summary information about the log entry.
Source: Displays the source of the communication.
Destination: Displays the destination of the communication.
Note: Displays the IP address of the communication

4.3.3 Log Setting

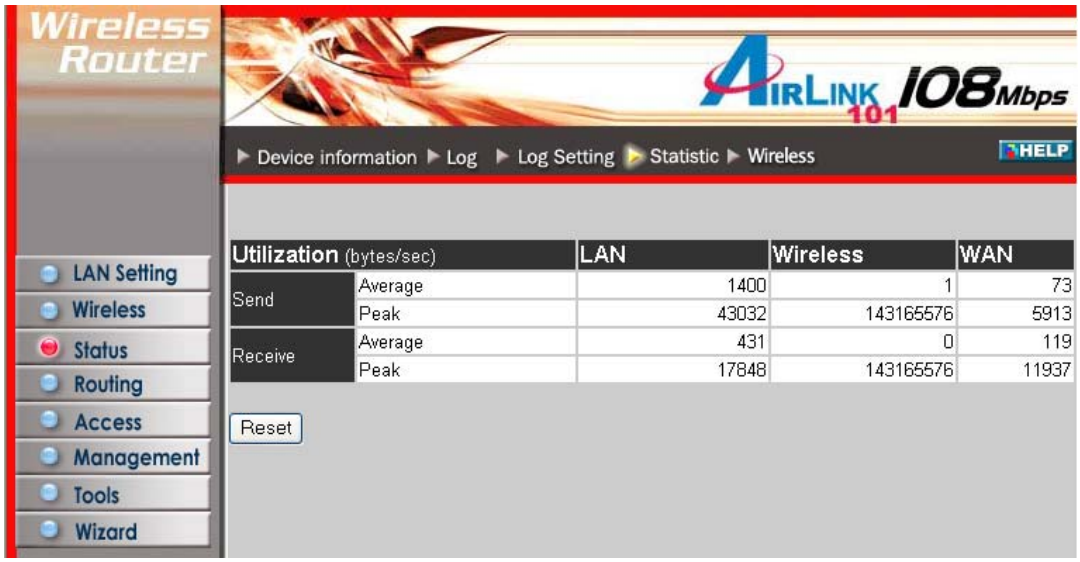
This screen enables you to set router logging parameters.



SMTP Server: Type the SMTP server address for the email that the log will be sent to in the next field.
Send to: Type an email address for the log to be sent to. Click ***Email Log Now*** to immediately send the current log.
Syslog Server: Type the IP address of the Syslog Server if you want the router to listen and receive incoming Syslog messages.
Log Type: Enables you to select what items to be included in the log:
● **System Activity:** Displays information related to router operation.
● **Debug Information:** Displays information related to errors and system malfunction.
● **Attacks:** Displays information about any malicious activity on the network.
● **Dropped Packets:** Displays information about packets that have not been transferred successfully.
● **Notice:** Displays important notices by the systems administrator.

4.3.4 Statistic

This screen displays a table that shows the rate of packet transmission via the router LAN and WAN ports (in bytes per second).



Click ***Reset*** to erase all statistics and begin logging statistics again.

4.3.5 Wireless

This screen enables you to view information about wireless devices that are connected to the router.

Connected Time: Displays how long the wireless device has been connected to the router.
MAC Address: Displays the MAC address of the connected wireless clients.

4.4 Routing

This section enables you to set how the router forwards data: Static and Dynamic. Routing Table enables you to view the information about the network topology created by the router.

4.4.1 Static

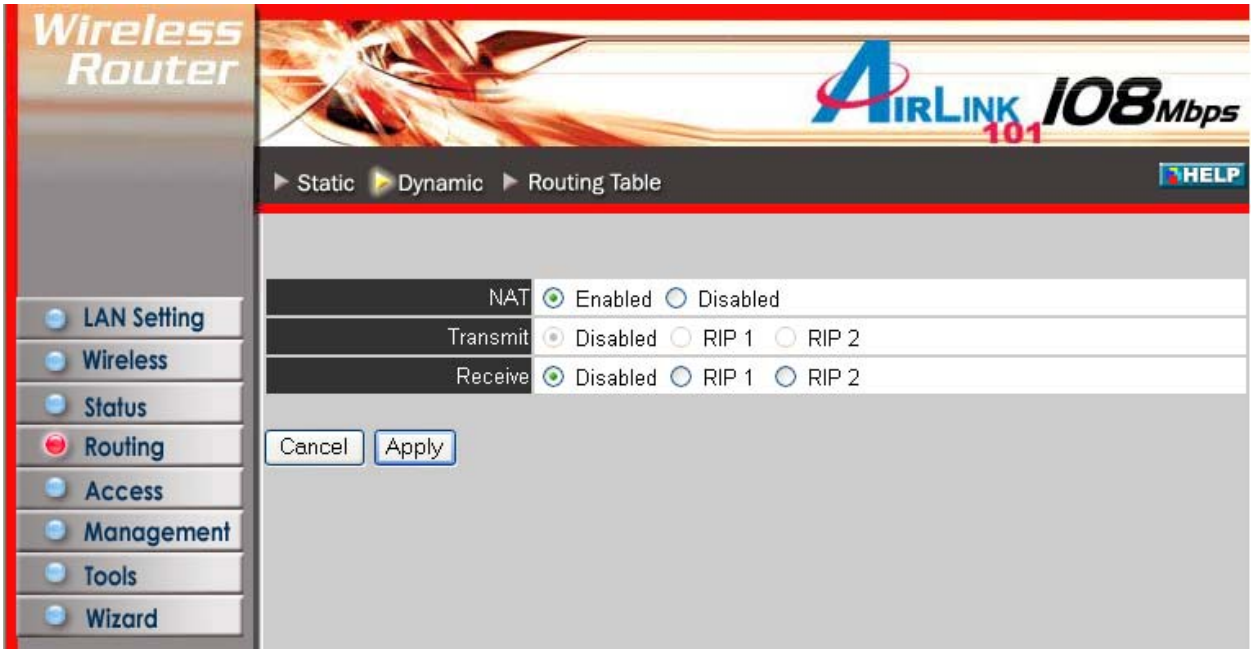
This page enables you to set parameters by which the router forwards data to its destination if your network has a static IP address.

Network Address: Type the static IP address your network uses to access the Internet. Your ISP or network administrator provides you with this information.
Network Mask: Type the network (subnet) mask for your network. If you do not type a value here, the network mask defaults to 255.255.255.255. Your ISP or network administrator provides you with this information.
Gateway Address: Type the gateway address for your network. Your ISP or network administrator provides you with this information.
Interface: Select which interface, WAN or LAN, you will use to connect to the Internet.
Metric: Select which metric you want to apply to this configuration.
Add: Click to add the configuration to the static IP address table at the bottom of the page.
Update: Select one of the entries in the static IP address table at the bottom of the page and, after changing parameters, click *Update* to confirm the changes.
Delete: Select one of the entries in the static IP address table at the bottom of the page and click *Delete* to remove the entry.

New: Click *New* to clear the text boxes and add required information to create a new entry.

4.4.2 Dynamic

This screen enables you to set NAT parameters.



NAT: Click the radio buttons to enable or disable NAT.
Transmit: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.
Receive: Click the radio buttons to set the desired transmit parameters, disabled, RIP 1, or RIP 2.

4.4.3 Routing Table

This screen enables you to view the routing table for the router. The routing table is a database created by the router that displays the network interconnection topology.

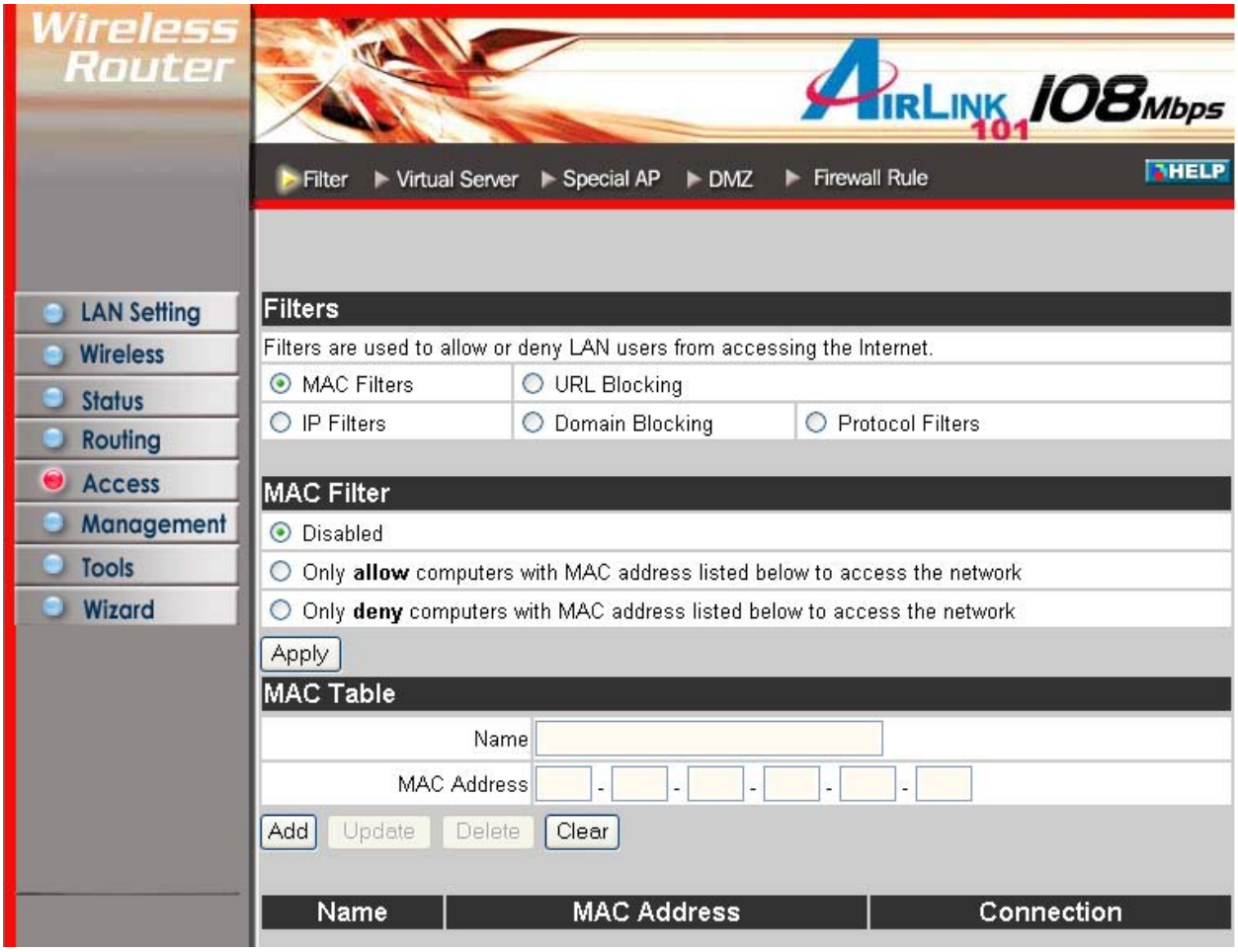
Network Address: Displays the network IP address of the connected node.
Network Mask: Displays the network (subnet) mask of the connected node.
Gateway Address: Displays the gateway address of the connected node.
Interface: Displays whether the node is connected via WAN or LAN.
Metric: Displays the metric of the connected node.
Type: Displays whether the node has a static or dynamic IP address

4.5 Access

This page enables you to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

4.5.1 MAC Filters

Enables you to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to *Disabled* to disable the MAC filter.

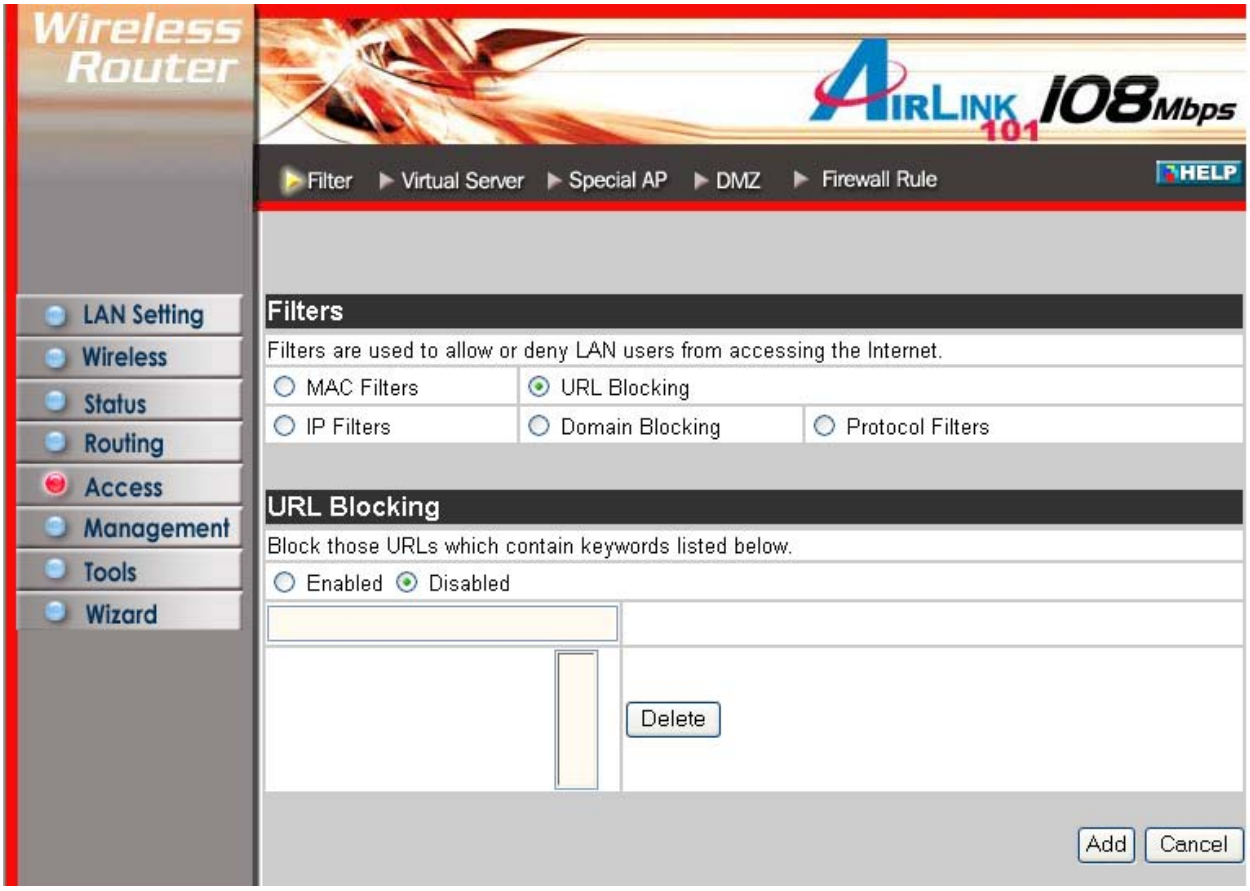


Disabled: Once the function of MAC filter is disabled, those listed in the MAC Table are allowed Internet access.
MAC Table: Use this section to specify which user is denied or allowed Internet access. The user profiles are listed in the table at the bottom of the page. **(*Note:*** Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit).
Name: Type the name of the user to be permitted/denied access.
MAC Address: Type the MAC address of the user's network interface.

Add: Click to add the user to the list at the bottom of the page.
Update: Click to update information for the user, if you have changed any of the fields.
Delete: Select a user from the table at the bottom of the list and click *Delete* to remove the user profile.

4.5.2 URL Blocking

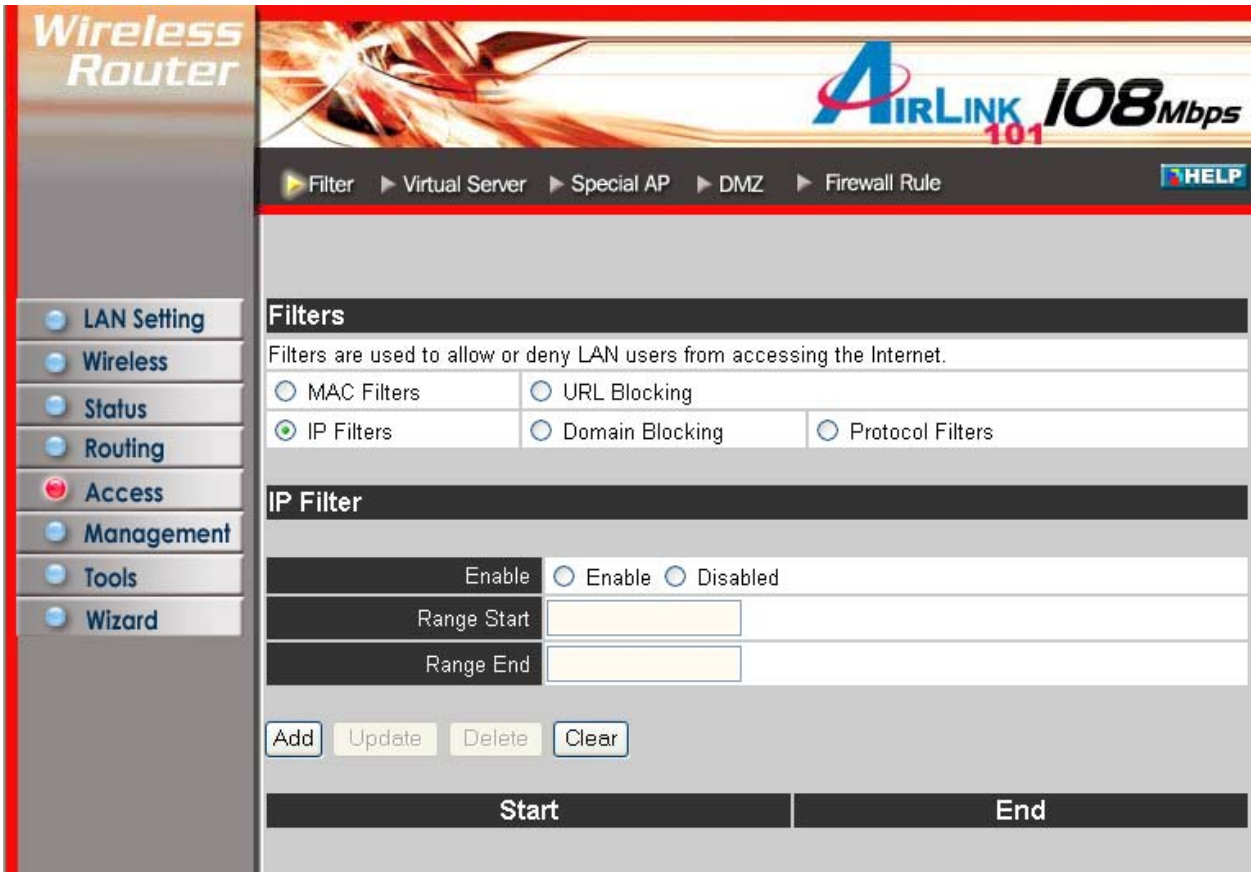
This page allows you to deny users from accessing certain URLs specified in the list.



Enabled/Disabled: Select to enable or disable URL blocking.
Once URL blocking is set to enabled, enter the keywords in the text field and click **Add**.
To delete a keyword, select it from the list and click **Delete**.

4.5.3 IP Filter

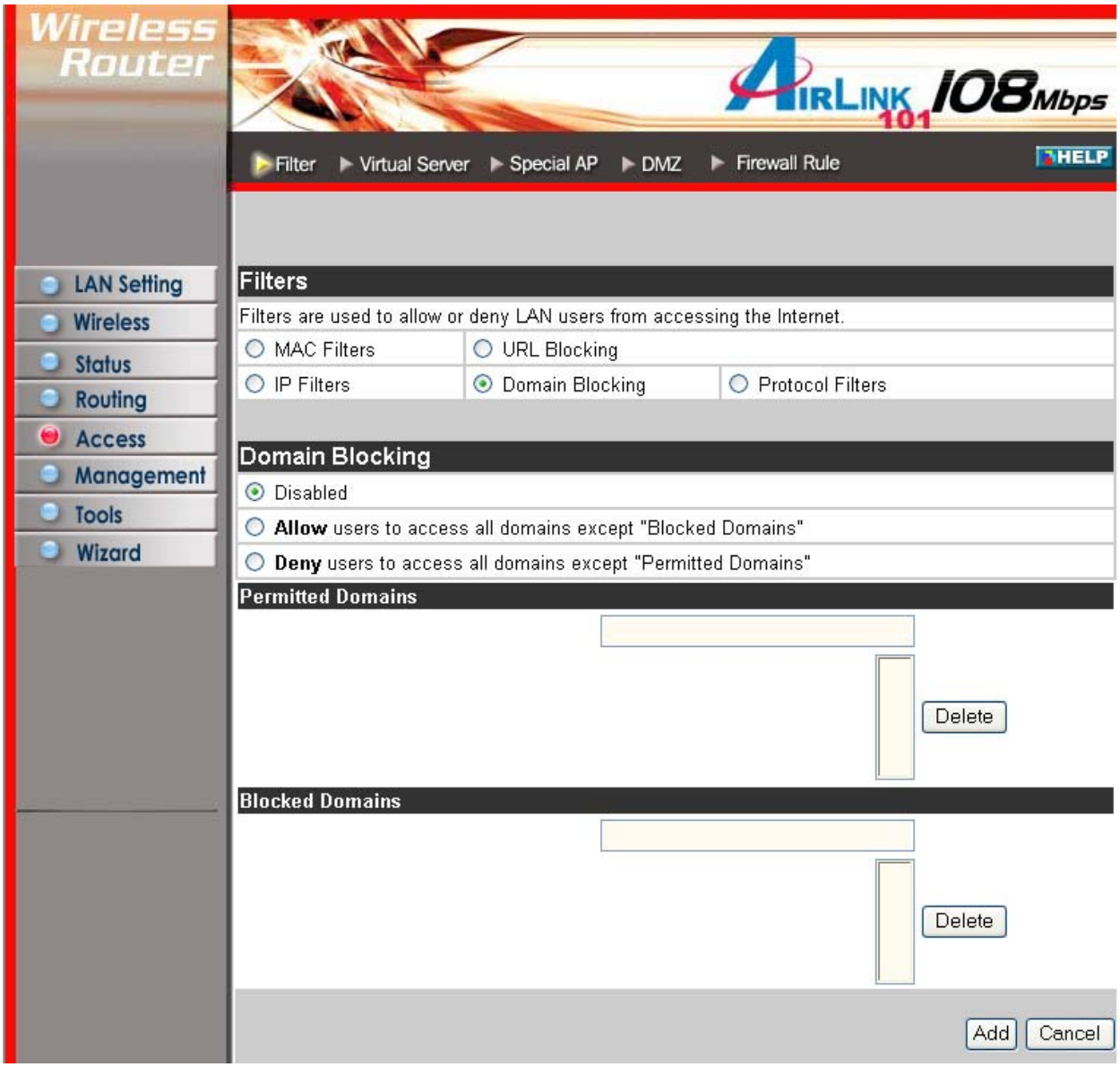
This screen enables you to define a minimum and maximum IP address range filter; all IP addresses falling in the range are not allowed Internet access. The IP filter profiles are listed in the table at the bottom of the page. (***Note*:** Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit).



Enable: Click to enable or disable the IP address filter.
Range Start: Type the beginning address for the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.
Range End: Type the final address for the IP range. IP addresses falling between this value and the Range Start are not allowed to access the Internet.
Add: Click to add the IP range to the table at the bottom of the screen.
Update: Click to update information for the range if you have selected a list item and have made changes.
Delete: Select a list item and click *Delete* to remove the item from the list.

4.5.4 Domain Blocking

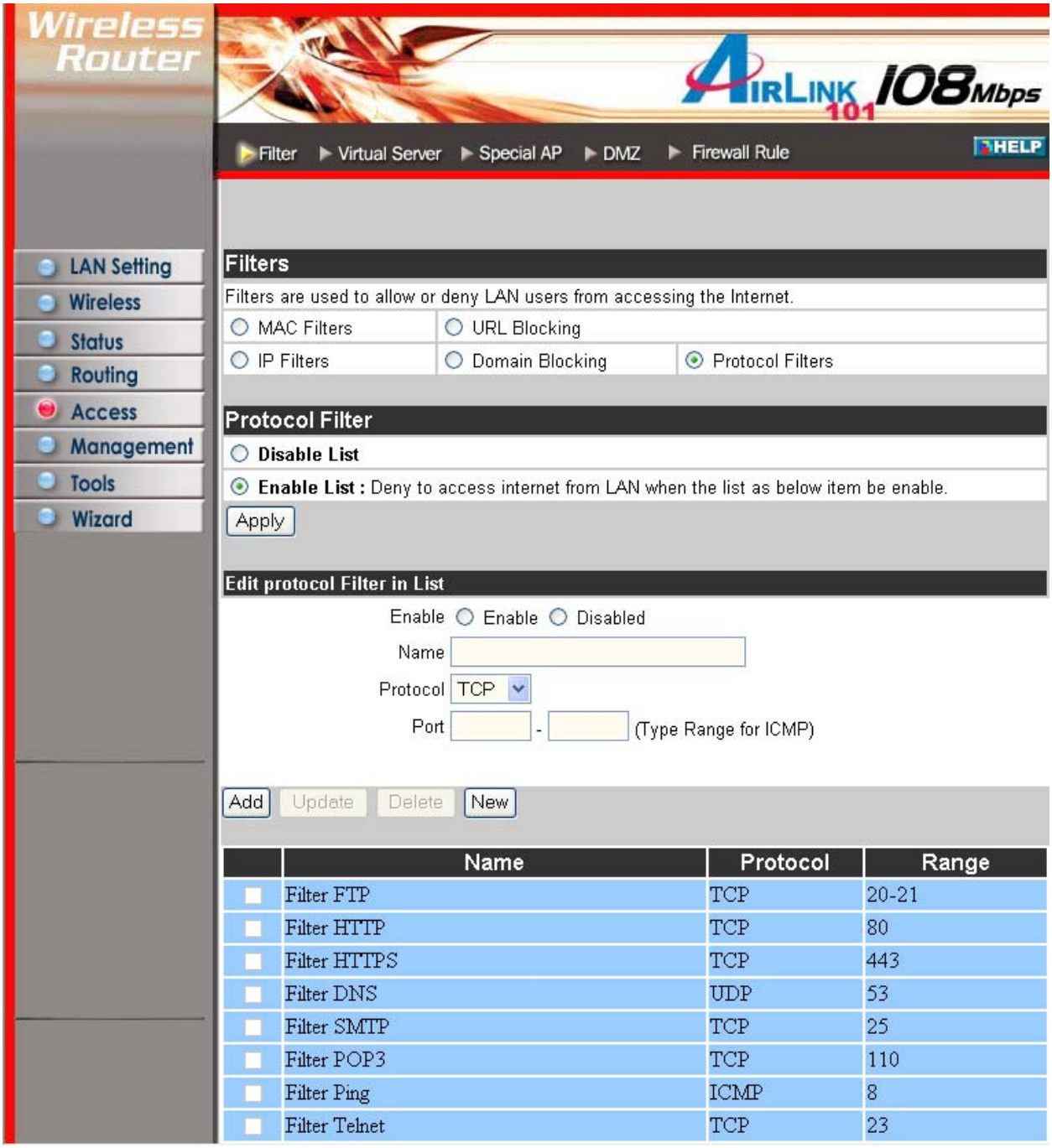
This page allows you to either permit or deny users from accessing certain domains specified in the list.



Domain Blocking: choose from Disabled, Allow users to access all domains except "Blocked Domains", or Deny users to access all domains except "Permitted Domains".
Permitted Domains: enter the domains you wish to allow access in this field and click **Add**.
Blocked Domains: enter the domains you wish to deny access in this field and click **Add**.

4.5.5 Protocol Filter

This screen enables you to allow and deny access based upon a communications protocol list you create. The protocol filter profiles are listed in the table at the bottom of the page.



Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit.

The most common protocols are listed in the table already. Select the protocol you wish to edit.

Protocol Filter:
Disable List: disables protocol filter
Enable List: enables protocol filter. If this is selected, the router will deny Internet access to those protocols that have the filter marked enabled.

Edit protocol filter in list:
Enable: protocol marked enabled will be denied access to the Internet.
Denied: protocol marked denied will be granted access to the Internet.

To edit a new protocol filter, click **New**. Edit the settings then click **Add**.

4.5.6 Virtual Server

This screen enables you to create a virtual server via the router. If the router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit.

Enable: Click to enable or disable the virtual server.
Name: Type a descriptive name for the virtual server.
Protocol: Select the protocol (TCP or UDP) you want to use for the virtual server.
Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.
Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.
LAN Server: Type the LAN IP address that will be assigned to the virtual server.
Add: Click to add the virtual server to the table at the bottom of the screen.
Update: Click to update information for the virtual server if you have selected a list item and have made changes.
Delete: Select a list item and click *Delete* to remove the item from the list.

4.5.7 Special AP

This screen enables you to specify special applications, such as games, that require multiple connections that are inhibited by NAT (i.e., if you need to open up certain ports for certain applications to access the Internet). The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit.

Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the router's WAN connection. Click **Disabled** on a profile to prevent users from accessing the application on the WAN.
Name: Type a descriptive name for the application.
Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.
● **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used to access the application.
● **Port Range:** Type the port range that can be used to access the application in the text boxes.
Incoming: Defines which incoming communications users are permitted to connect with.
● **Protocol:** Select the protocol (TCP, UDP, or ICMP) that can be used by the incoming communication.
● **Port:** Type the port number that can be used for the incoming communication.
Add: Click to add the special application profile to the table at the bottom of the screen.
Update: Click to update information for the special application if you have selected a list item and have made changes.
Delete: Select a list item and click *Delete* to remove the item from the list.

4.5.8 DMZ

This screen enables you to create a DMZ for a computer that cannot access the Internet applications properly through the router and its associated security settings. It allows the specified computer to have unrestricted two-way access with the Internet.

Note: Any client added to the DMZ exposes the client to security risks such as viruses and unauthorized access.

Enable: Click to enable or disable DMZ.

DMZ Host IP: Type the IP address of the computer. The computer with the specified IP address will have unrestricted two-way access with the Internet.
Apply: Click to save the settings.

4.5.9 Firewall Rule

This screen enables you to set up the firewall. The router provides basic firewall functions by filtering all the packets that enter the router using a set of rules. The rules are in an ordered sequence—the higher a rule is in the list, the higher the priority the rule has.

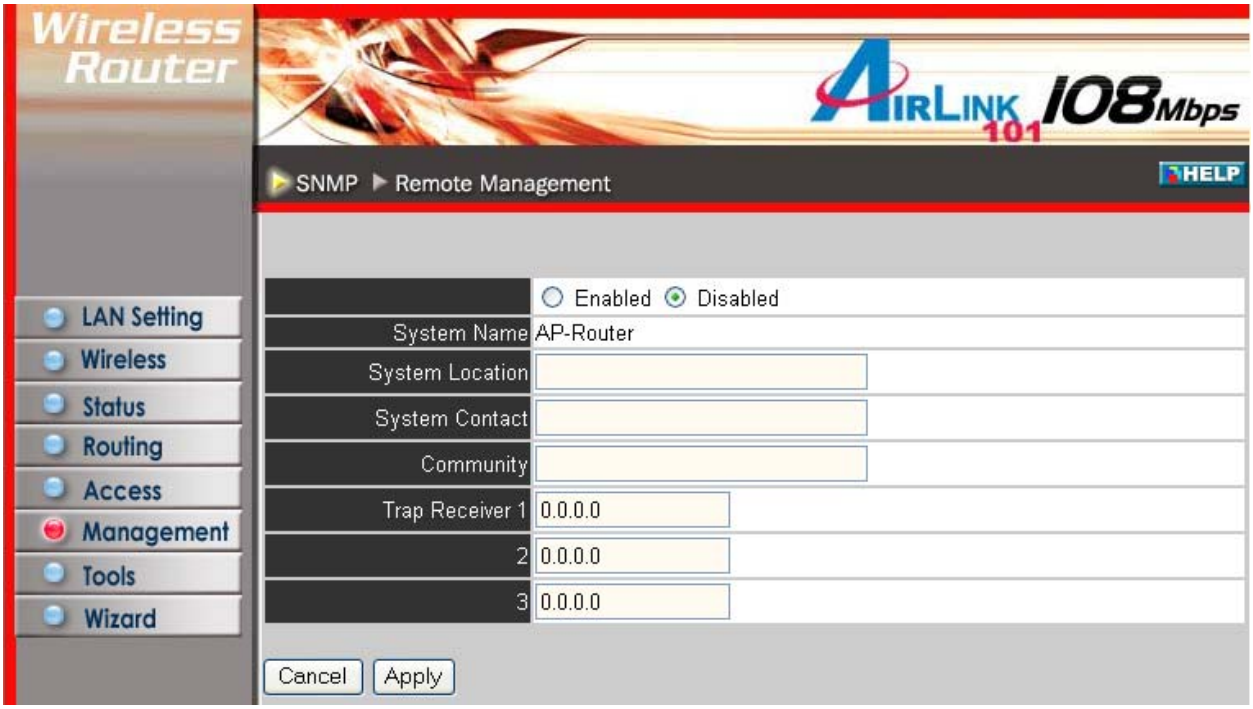
Enable: Click to enable or disable the firewall rule profile.
Name: Type a descriptive name for the firewall rule profile.
Action: Select whether to allow or deny packets that conform to the rule.
Source: Defines the source of the incoming packet that the rule is applied to.
● **Interface:** Select which interface (WAN or LAN) the rule is applied to.
● **IP Range Start:** Type the beginning of the IP address range that the rule is applied to.
● **IP Range End:** Type the end of the IP address range that the rule is applied to.
Destination: Defines the destination of the incoming packet that the rule is applied to.
● **Interface:** Select which interface (WAN or LAN) the rule is applied to.
● **IP Range Start:** Type the beginning of the IP address range that the rule is applied to.
● **IP Range End:** Type the end of the IP address range that the rule is applied to.
● **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
● **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.
Update: Click to update information for the rule if you have selected a list item and have made changes.
Delete: Select a list item and click ***Delete*** to remove the item from the list.
New: Click ***New*** to erase all fields and enter new information.
Priority Up: Select a rule from the list and click ***Priority Up*** to increase the priority of the rule.
Priority Down: Select a rule from the list and click ***Priority Down*** to decrease the priority of the rule.
Update Priority: After increasing or decreasing the priority of a rule, click ***Update Priority*** to save the changes.

4.6 Management

4.6.1 SNMP

This screen enables you to configure SNMP.

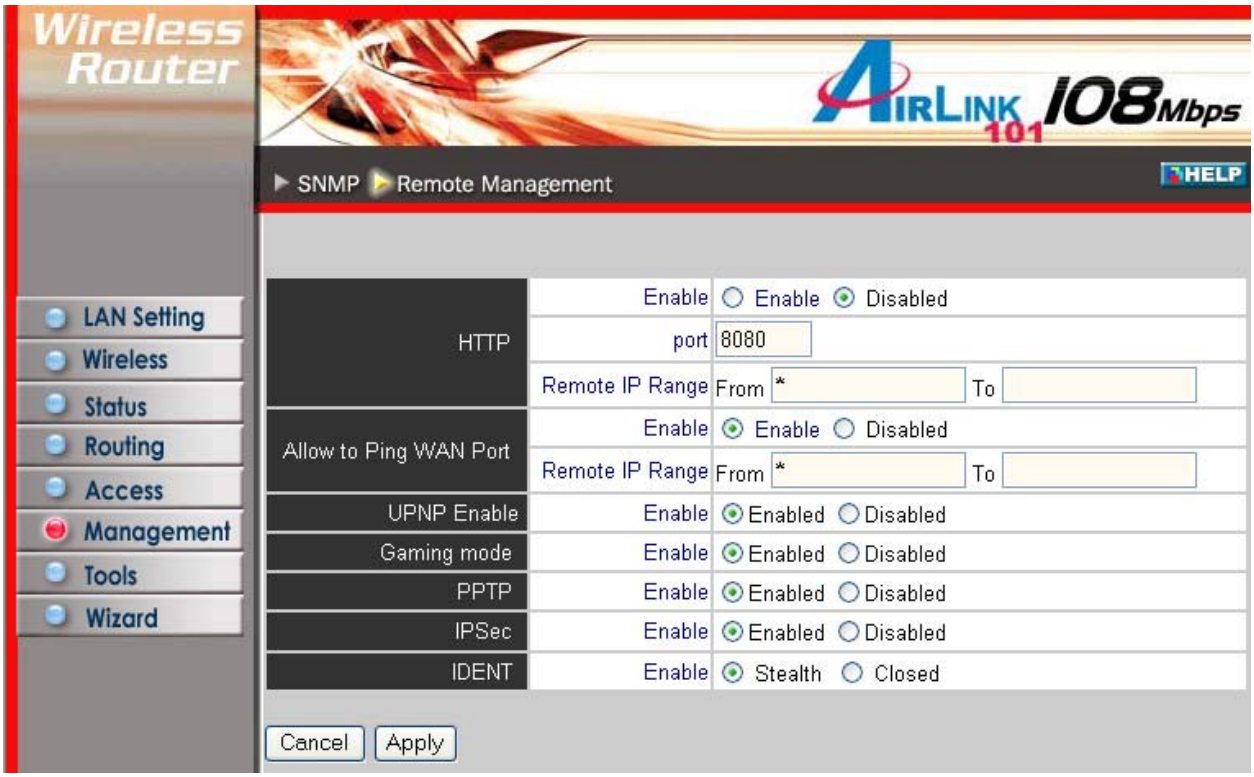


Enabled/Disabled: Click to enable or disable SNMP.
System Name: Displays the name given to the router.
System Location: Displays the location of the router (normally, the DNS name).
System Contact: Displays the contact information for the person responsible for the router.

Community: SNMP system name for exchanging SNMP community messages. The name can be used to limit SNMP messages passing through the network. The default name is 'public.'
Trap Receiver: Type the name of the destination PC that will receive trap messages.

4.6.2 Remote Management

This screen enables you to set up remote management. Using remote management, the router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.



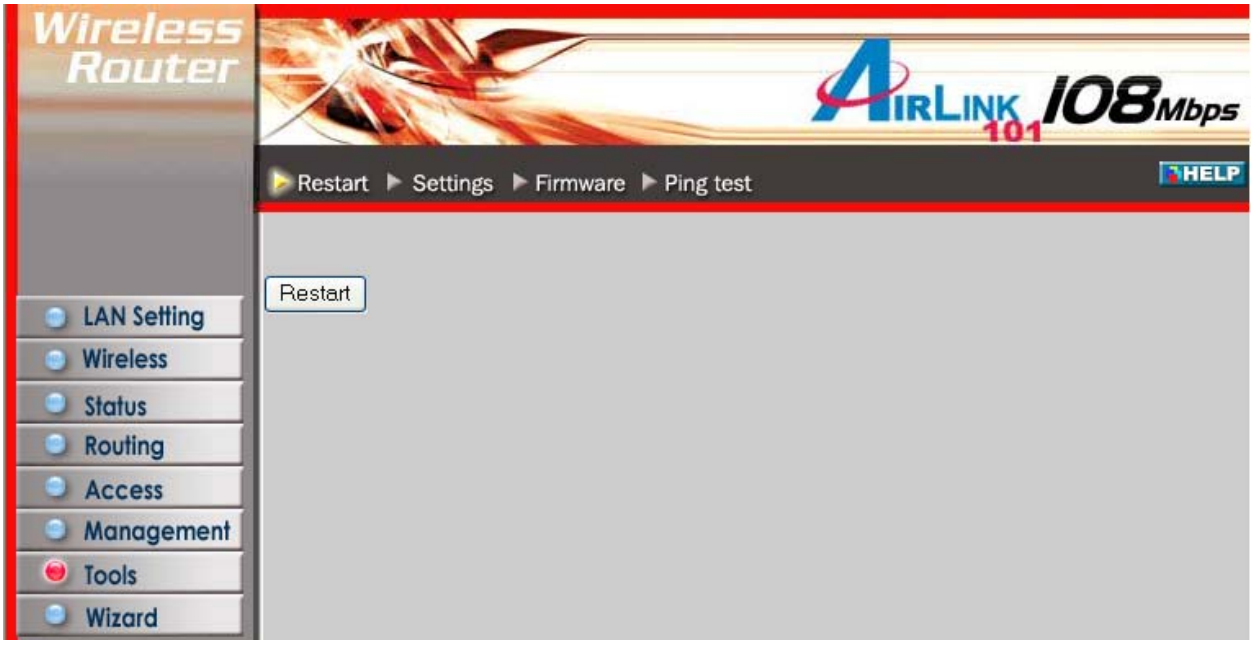
HTTP: Select to enable or disable remote management.
Port: enter a port number for the remote management. Default is **8080**.
Remote IP Range: Specify the IP range of remote addresses that can manage the router.
Allow to Ping WAN Port: Select to enable or disable ping response from WAN port.
Remote IP Range: Specify the IP range of remote addresses that the router will respond to ping requests.
UPNP: UPNP is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The Router is an UPnP enabled router and will only work with other UPnP devices/software. If you do not want to use the UPnP functionality, it can be disabled by selecting "Disabled".
Gaming Mode: If you are experiencing difficulties when playing online games or even certain applications that use voice data, you may need to enable Gaming Mode for

these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode be disabled.
PPTP: Enables you to set up PPTP access for remote management.
IPSec: Enables you to set up IPSec access for remote management.
IDENT: Choose to close or stealth port 113.

4.7 Tools

This page enables you to restart the router, save and load different settings as profiles, restore factory default settings, upgrade the firmware, and ping remote IP addresses.

4.7.1 Restart



Click ***Restart*** to restart the router in the event the router is not performing correctly.

4.7.2 Settings

This screen enables you to save your settings as a profile and load the profiles for different circumstances. You can also load the factory default settings.

Save Settings: After you have configured all the settings, click **Save** to save the current configuration as a profile so that you can load it when necessary.
Load Settings: Click ***Browse*** and go to the location of a stored profile. Click ***Load*** to load the profile's settings.
Restore Factory Default Settings: Click to restore the factory default settings. All configuration changes you have made will be lost.

4.7.3 Firmware

This screen enables you to keep the router firmware up to date.

Please follow the instructions below:
1. Download the latest firmware from the manufacturer's web site and save it to your disk.
2. Unzip the downloaded file.
3. Click ***Browse*** and go to the location of the unzipped firmware file.
4. Select the file and click **Upgrade** to update the firmware to the latest release.
5. Verify the firmware is updated by reviewing the firmware version on the **Status** page.

4.7.4 Ping Test

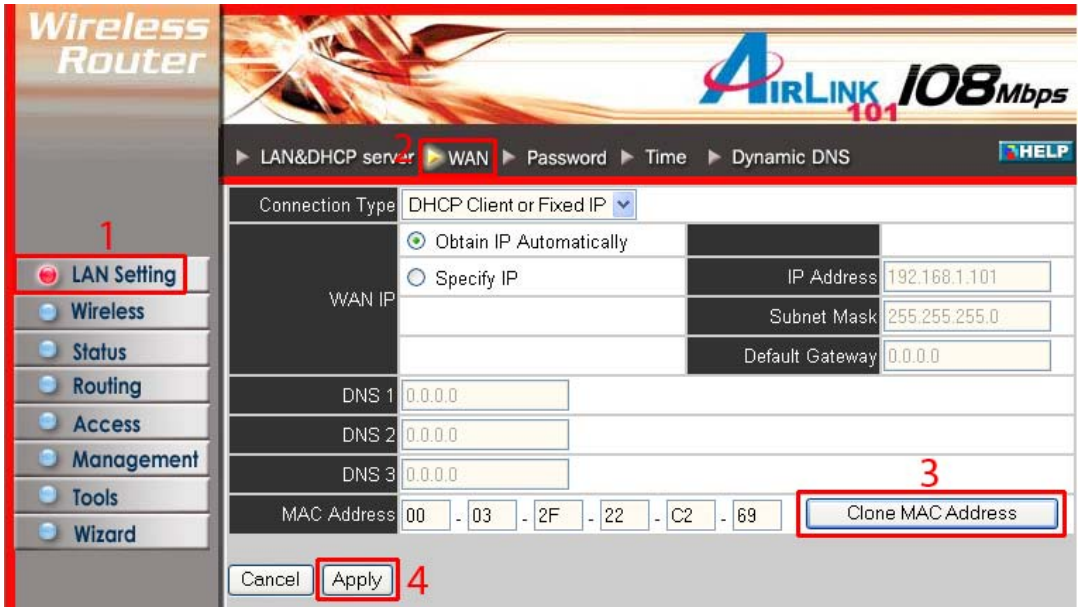
The ping test enables you to determine whether an IP address or host is present on the Internet.

Type the host name or IP address in the text box and click **Ping**.

5. Troubleshooting

For Cable Modem Users Only

Step 1 Log into the router's **LAN Setting** page and click **WAN**.



Step 2 Click **Clone MAC Address**, and click **Apply**.

Step 3 Redo the Setup Wizard.

Step 4 Verify the **Connection Status** as described in **Section 3, Verifying Internet Connection**.

For DSL Users Only

Step 1 Go to the router's Setup Wizard.

Step 2 At the PPPoE setting, double-check the spelling of your User name and Password. Some ISP's require you to include the domain name along with your User name for the User name field.

Example: **username@sbcglobal.net**

Step 3 Complete the Setup Wizard and then verify the **Connection Status** as described in **Section 3, Verifying Internet Connection**.

For Cable Modem and DSL Users

Step 1 Power off the Cable/DSL modem, router, and computer and wait for **5 minutes**.

Step 2 Turn on the Cable/DSL modem and wait for the lights on the modem to settle down.

Step 3 Turn on the router and wait for the lights on the router to settle down.

Step 4 Turn on the computer.

Step 5 Redo the Setup Wizard.

Step 6 Verify the Connection Status as described in **Section 3, Verifying Internet Connection**.

Appendix

Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Web Site: www.airlink101.com